Guida per l'utente

12.0

MDaemon Email Server
Guida per l'utente

v12.0.0 - January 2011

Sommario

Sezione I

1 MDaemon Email Server 12.0

1.1 Introduzione

Introduzione

MDaemon Email Server di Alt-N Technologies v12.0 è un server di posta SMTP/POP3/IMAP basato su standard che supporta i sistemi Windows 7/Vista/XP/2008/2003 offrendo una gamma completa di funzioni. Dotato di un'ampia suite di potenti strumenti integrati per la gestione di account di posta e dei vari formati di messaggistica, MDaemon è stato progettato per rispondere alle esigenze di posta elettronica di un numero illimitato di utenti. MDaemon include un server di posta scalabile per sessioni SMTP, POP3 e IMAP4, comprensivo di supporto LDAP e Active Directory, un client e-mail basato su browser, strumenti di filtro dei contenuti e della posta indesiderata (spam), avanzate funzioni di sicurezza e molto altro ancora.

MDaemon Standard, PRO e FREE

Il server e-mail MDaemon è disponibile in tre versioni: MDaemon Standard, PRO e FREE. Grazie alle potenti funzionalità di MDaemon Standard, è possibile gestire i messaggi di posta dell'intera rete nel server SMTP di MDaemon o raccogliere la posta dell'intero dominio da una sola casella postale POP3 fornita dall'ISP mediante la funzione DomainPOP. È inoltre possibile ospitare più liste di distribuzione, consentendo l'accesso degli utenti ai messaggi e-mail mediante il componente di posta Web WorldClient e utilizzare numerose altre funzioni. MDaemon PRO include tutte le funzioni della versione Standard e offre inoltre il supporto per IMAP4, per i domini multipli, per la condivisione di dominio, per i gateway, per le liste di distribuzione estese e per l'integrazione con gli smartphone BlackBerry che lo rendono ideale per aziende di grandi dimensioni e con esigenze maggiori. MDaemon PRO aggiunge inoltre funzioni di calendario e pianificazione di gruppo, un sistema di messaggistica istantanea, il supporto multilingua per WorldClient, la creazione automatica di gateway di dominio e molto altro ancora. MDaemon FREE è una versione limitata, ma completamente gratuita, di MDaemon che

mira a fornire le funzioni di base del server di posta per un massimo di cinque utenti rivelandosi, così, perfetto per abitazioni o per piccole aziende che desiderino un server di posta affidabile che possa tenere il passo con la propria attività. MDaemon FREE supporta i protocolli SMTP e POP3, comprende il componente di posta Web WorldClient, il supporto per l'amministrazione remota e numerose altre funzioni. Per uno schema grafico dettagliato con la descrizione delle funzioni di ogni versione, visitare: www.altn.com.

Funzioni di MDaemon

Oltre alla gestione della posta SMTP, POP3 e IMAP4, MDaemon offre numerose altre funzionalità. Di seguito è riportato un elenco di alcune funzioni di MDaemon.

- MDaemon Pro include un server BES perfettamente integrato che consente agli utenti di sincronizzare la posta, il calendario, i contatti e altri dati PIM di MDaemon con un dispositivo BlackBerry.
- Supporto completo della scansione e protezione anti-virus mediante SecurityPlus per MDaemon. Questo componente aggiuntivo di MDaemon è un efficace antivirus. Consente infatti di eseguire la scansione dei messaggi e di ripulirli o eliminarli automaticamente prima che raggiungano i destinatari. Inoltre, è possibile configurare MDaemon per l'invio di un messaggio di notifica del virus all'amministratore, al mittente e al destinatario di un messaggio infettato. SecurityPlus per MDaemon è un prodotto concesso in licenza separatamente, disponibile presso www.altn.com.
- MDaemon offre una completa suite di servizi per la gestione delle liste di distribuzione e dei gruppi di posta elettronica e consente quindi di creare un numero illimitato di liste di distribuzione diverse, che possono contenere contatti locali e/o remoti. È possibile impostare i parametri delle liste di distribuzione in modo da consentire o rifiutare le richieste di iscrizione, definire il tipo di lista (pubblica o privata), inviare risposte sia alla lista sia al mittente del messaggio, ricevere i messaggi in formato riassunto e configurare una serie di altre funzioni.
- WorldClient è un componente integrato di MDaemon che consente agli utenti di una rete di accedere alla posta elettronica utilizzando un browser Web anziché il client di posta elettronica specifico di una postazione. Questo strumento è ideale per gli utenti che non dispongono di un computer dedicato da cui controllare le proprie e-mail.
- WorldClient è un client e-mail dotato di una suite completa di funzioni che consentono di effettuare le seguenti operazioni: inviare e ricevere messaggi, eseguirne il controllo ortografico, gestire la posta elettronica in più cartelle personali, visualizzare l'interfaccia in 18 lingue, pianificare riunioni e appuntamenti nonché condividere il calendario e le attività con altri utenti, amministrare le impostazioni degli account (se utilizzato insieme a WebAdmin), gestire i contatti e molto altro ancora. WorldClient comprende inoltre ComAgent, una piccola utilità che è possibile scaricare e installare nel computer locale di un utente. Questa utilità consente di accedere facilmente a messaggi e a cartelle e di controllare la posta senza aprire il browser Web. Infine, WorldClient include un sistema completo di messaggistica istantanea (o IM, Instant Messaging) utilizzabile per comunicare rapidamente con gli utenti di MDaemon/WorldClient.
- MDaemon è dotato di numerose funzioni, ideate appositamente per rendere sicuro il sistema di posta elettronica. Le funzioni Spam Filter e Liste nere DNS,

rispettivamente per il filtro della posta indesiderata e per la creazione di liste nere dei DNS, consentono di evitare o limitare la ricezione di messaggi spam indirizzati verso o attraverso un dominio. Le funzioni Vaglio IP, Vaglio host e Lista nera indirizzi offrono la possibilità di eseguire analisi e di impedire che determinati indirizzi o domini si colleghino o inviino messaggi attraverso il sistema. Queste funzioni, inoltre, permettono di collegarsi a determinati indirizzi IP controllando al contempo tutti gli altri.

- Grazie al supporto per il protocollo LDAP (Lightweight Directory Access Protocol), MDaemon consente di mantenere un server LDAP costantemente aggiornato su tutti gli account degli utenti. Questa funzione rende possibile la gestione di una rubrica di indirizzi LDAP aggiornata, alla quale possono accedere gli utenti che utilizzano client di e-mail compatibili con LDAP. Inoltre, è possibile utilizzare come database utenti di MDaemon Active Directory o un server LDAP anziché un database compatibile con ODBC o il sistema `USERLIST.DAT` locale. Questa possibilità consente di configurare più server MDaemon in più postazioni in modo da condividere il medesimo database utenti.

- Le complete funzionalità di analisi di MDaemon consentono di usufruire di un servizio di posta elettronica per un'intera LAN mediante un'unica casella postale POP3, con accesso remoto via ISP. In questo modo è possibile utilizzare un servizio di posta elettronica per un'intera rete, a un costo molto più contenuto rispetto a quello normalmente richiesto.

- È possibile configurare MDaemon in modo da mantenere sempre aggiornate le informazioni sugli utenti con l'archivio contatti di Microsoft Outlook o con la rubrica di Windows. In questo modo, è possibile usufruire di un ulteriore strumento per rendere disponibile a tutti gli utenti della rete la rubrica di indirizzi globale.

- Gli alias di indirizzo consentono di instradare i messaggi di posta elettronica indirizzati a caselle postali "fittizie" verso account o liste di distribuzione validi. Grazie a tale funzione, è possibile assegnare più indirizzi e-mail a un singolo account e a una singola lista presso uno o più domini.

- La funzione Gateway di dominio offre l'opportunità di impostare domini separati per gruppi o reparti diversi, sia locali all'interno della rete, sia esterni su Internet. Questa funzione fa sì che tutta la posta indirizzata verso un dominio per cui il server MDaemon funge da gateway venga inviata da MDaemon alla casella postale di quel dominio. In questo modo, è possibile raccogliere la posta dal server MDaemon o dal client di posta del dominio in questione e ridistribuirla fra gli utenti del dominio. Questa funzionalità può essere inoltre utilizzata per utilizzare MDaemon come server di posta di backup per altri domini.

- Mediante messaggi e-mail in formato speciale, è possibile controllare gli account in modalità remota. Questa funzionalità offre una notevole flessibilità di gestione e notevoli vantaggi per gli utenti, che possono gestire in modo autonomo le semplici operazioni di manutenzione quotidiana dell'account, ad esempio la modifica della password.

- Gestione remota integrata basata su Web tramite WebAdmin. WebAdmin è integrato con MDaemon e WorldClient e consente agli utenti di esaminare e modificare le impostazioni degli account tramite un browser Web. È possibile definire le impostazioni che possono essere modificate direttamente dagli utenti, nonché assegnare un'autorizzazione di accesso per ogni account. WebAdmin può

essere inoltre utilizzato dall'amministratore (e da un utente con pari privilegi) per controllare o modificare qualunque impostazione di MDaemon e qualsiasi file per cui sia stato autorizzato il controllo mediante il sistema WebAdmin.

- Mediante la funzione Cataloghi file, l'amministratore della posta elettronica ha la possibilità di creare gruppi di file protetti da password che vengono codificati e inviati automaticamente agli utenti utilizzando messaggi e-mail in formato speciale.
- Un sistema interno di trasporto dei messaggi, noto come RAW, costituisce un semplice metodo per trasmettere i messaggi nel flusso della posta, semplificando notevolmente lo sviluppo di software di posta personalizzato. Grazie al sistema RAW è possibile disporre di un sistema completo di posta, utilizzando un semplice editor di testo e una coppia di file batch.
- Un sistema di filtro dei contenuti molto versatile consente di personalizzare il comportamento del server in base al contenuto dei messaggi e-mail in entrata e in uscita. È possibile inserire e aggiungere intestazioni di messaggio, aggiungere piè di pagina ai messaggi, rimuovere gli allegati, inoltrare copie ad altri utenti, attivare l'invio automatico di un messaggio istantaneo, eseguire programmi e altro ancora.

Requisiti di sistema

Per informazioni aggiornate sui requisiti di sistema e per consigli su MDaemon, visitare la pagina Requisiti di sistema all'indirizzo www.altn.com.

Vedere:

Novità di MDaemon 12.0 15
Aggiornamento a MDaemon 12.0 24
Schermata principale di MDaemon 28
Guida 20

1.2 Novità di MDaemon 12.0

BES BlackBerry 165

MDaemon Pro è dotato di un server BES integrato e personalizzato, ideato espressamente per la distribuzione e l'utilizzo con MDaemon. Il server BES consente agli utenti di sincronizzare i messaggi di posta elettronica, il calendario e altri dati PIM (Personal Information Management) di MDaemon/WorldClient con gli smartphone BlackBerry. BES consente inoltre di impostare criteri di sicurezza sui dispositivi degli utenti e perfino di cancellare i dati da un dispositivo in caso di smarrimento o di furto.

Le funzionalità BES di MDaemon sono elencate di seguito.

- Nessuna necessità di client di sincronizzazione di terze parti. I dati dei singoli utenti vengono sincronizzati mediante il software già presente in tutti i dispositivi BlackBerry.

- I messaggi di posta elettronica di MDaemon/WorldClient, incluse le cartelle di posta, vengono sincronizzati con il dispositivo in entrambe le direzioni. Pertanto le operazioni di lettura, spostamento, eliminazione e così via della posta, sono sincronizzate sia sul dispositivo che sul server ovunque si siano verificate.
- Sincronizzazione bidirezionale del calendario. Se ad esempio si crea un nuovo appuntamento, si imposta un promemoria o si modifica un appuntamento sul dispositivo o in WorldClient, l'operazione viene sincronizzata su entrambi.
- Sincronizzazione bidirezionale delle attività e delle note.
- Ricerca nella rubrica globale.
- Pianificazione della disponibilità (Free/Busy).
- Supporto limitato dei criteri dei dispositivi BlackBerry che consente l'impostazione di criteri quali: richiesta della password, scadenza della password, crittografia dei file multimediali e altro ancora.
- Impostazione di criteri diversi per i singoli domini o utenti.
- Modifica remota della password e blocco del dispositivo.
- Cancellazione dei dati dal dispositivo in caso, ad esempio, di smarrimento o furto.
- Opzioni di backup e di ripristino del database BES.

Le principali opzioni BES di MDaemon si trovano in: Impostazioni » BlackBerry... » BES BlackBerry 165, mentre le opzioni specifiche per gli account si trovano nella schermata BES BlackBerry 350 di Account Editor.

ActiveSync per MDaemon 137

MDaemon supporta anche "ActiveSync per MDaemon," un server ActiveSync (AirSync) con una licenza OTA concessa separatamente. Questo server è in grado di sincronizzare il calendario e i contatti predefiniti dell'utente tra l'account MDaemon/WorldClient e un dispositivo ActiveSync. Le opzioni ActiveSync di MDaemon si trovano in: Impostazioni » Web, Sincronizzazione e Servizi IM... » ActiveSync 137 e un'opzione nella schermata Opzioni 374 di Account Editor consente di disabilitarle per alcuni utenti. La schermata ActiveSync include opzioni relative all'attivazione o alla disattivazione dell'opzione per i singoli domini, all'impostazione del valore di timeout della sessione e all'indicazione del livello di dettaglio delle registrazioni ActiveSync. Include inoltre collegamenti alle istruzioni di configurazione dei dispositivi per l'utilizzo di ActiveSync.

Alla prima attivazione per MDaemon, ActiveSync offre 30 giorni in modalità di prova. In seguito, per continuare a utilizzarlo, è necessario acquistare la licenza pagandone il costo un'unica volta. È possibile acquistare la chiave di licenza presso www.altn.com o presso il proprio rivenditore/distributore locale.

Miglioramenti di WorldClient

- Le chat di ComAgent ora sono incluse nel tema LookOut. Quando si attiva questa funzione da una nuova opzione della pagina Personalizza di WorldClient, nell'angolo inferiore destro del browser viene visualizzata la barra di ComAgent. Ciò consente di visualizzare un elenco di amici e di comunicare con gli amici ComAgent analogamente a quanto avverrebbe con le altre applicazioni

ComAgent.

- Editor WYSIWYG aggiornato. Questa caratteristica offre migliori prestazioni sui tempi di caricamento della composizione dei messaggi e include miglioramenti e correzioni sia per la creazione che per la composizione dei messaggi.
- Il calendario del tema LookOut di WorldClient è stato ridisegnato per consentire un migliore rendering degli eventi e per offrire un'interazione più simile a quella con il desktop.
- Ora è possibile modificare le singole occorrenze di un evento ricorrente del calendario di WorldClient.
- I temi del desktop possono disporre di una colonna To (A). Attivando questa opzione, con la colonna Sender (Mittente) viene sempre visualizzato anche il campo From (Da). In precedenza, la colonna From poteva diventare To o From, in base al fatto che l'utente si trovasse nella cartella Posta inviata. Gli utenti possono attivare questa colonna in Opzioni » Colonne di WorldClient.

Altre funzioni e modifiche

MDaemon 12.0 dispone di numerose funzioni e modifiche. Per un elenco completo delle nuove funzioni, delle modifiche e delle correzioni rispetto alle precedenti versioni di MDaemon, vedere il file `RelNotes.html` nella sottocartella `\Docs\` di MDaemon.

Novità di MDaemon 11

Integrazione con i servizi Internet BlackBerry (BIS) (solo MDaemon PRO) 184

MDaemon offre il supporto diretto per i servizi Internet BlackBerry (BIS). Gli utenti BIS possono integrare l'account di posta di MDaemon con il proprio smartphone BlackBerry, inviare la posta tramite BlackBerry e gestire la posta con funzioni avanzate utilizzando un dispositivo BlackBerry e MDaemon. I dispositivi BlackBerry configurati per ricevere la posta da MDaemon tramite IMAP o POP nelle versioni di MDaemon precedenti alla 11.0 possono ora essere impostati per inviarla. I messaggi composti sul dispositivo, inoltre, vengono inviati a MDaemon per la consegna, senza utilizzare i server BIS. In tal modo, i messaggi di posta elettronica composti con un dispositivo BlackBerry saranno conformi ai criteri di protezione, alle regole di filtro dei contenuti, alla tecnologia DKIM, ai criteri di archiviazione e alle altre configurazioni implementate nel server dell'organizzazione.

Poiché i servizi BIS consentono di raccogliere la posta solo dalla casella Posta in arrivo degli utenti, si potrebbero verificare problemi se si utilizzano filtri IMAP 353 per ordinare automaticamente i messaggi in cartelle specifiche. Per risolvere il problema, la schermata BIS BlackBerry 352 di Account Editor e la pagina Cartelle di WorldClient consentono, rispettivamente, agli amministratori e agli utenti di selezionare le cartelle che contengono i nuovi messaggi da recapitare al dispositivo. Quando il server BIS si connette a MDaemon per raccogliere i nuovi messaggi dalla Posta in arrivo dell'utente, MDaemon invia anche i nuovi messaggi delle cartelle selezionate. Tutti i nuovi messaggi delle cartelle selezionate vengono inviati alla Posta in arrivo del dispositivo BlackBerry.

In tal modo, al dispositivo non vengono inviate le cartelle intere, ma solo i nuovi messaggi.

Infine, uno schema di gestione degli alias delle cartelle interne consente di assegnare alle cartelle "Posta inviata" e "Posta eliminata" di ogni utente valori riconosciuti da BIS, indipendentemente dal nome assegnato alle cartelle nell'account dell'utente. Ciò consente di collocare la posta inviata ed eliminata nelle cartelle di MDaemon appropriate.

Routing intelligente dei messaggi 42

Questa nuova opzione che consente il routing intelligente dei messaggi è stata inserita nella schermata Consegna 42 della finestra di dialogo Dominio predefinito/server. Per impostazione predefinita, quando è possibile MDaemon conserva una sola copia di ogni messaggio inviato a più destinatari e utilizza più comandi RCPT per consegnare il messaggio. Ciò consente di risparmiare spazio su disco e larghezza di banda. Se selezionata, ad esempio, questa opzione è attiva ogni volta che un singolo messaggio viene indirizzato a più destinatari dello stesso dominio. Se inoltre si utilizza l'opzione di consegna "*Invia i messaggi in uscita al server indicato*", che consente di inviare la posta in uscita al solo host indicato, MDaemon archivia una singola copia di ogni messaggio e utilizza più comandi RCPT anche se i destinatari appartengono a domini diversi.

Supporto Sync Client migliorato 135

È stato aggiunto il supporto per il client open source Funambol SyncML versione 8.0. Il client è disponibile gratuitamente ed è stato notevolmente migliorato rispetto alle versioni precedenti. In particolare, il client BlackBerry offre quanto promesso.

Collegamento allegati (solo MDaemon PRO) 154

La funzione Collegamento allegati consente di rimuovere gli allegati dai messaggi di posta elettronica e di memorizzarli localmente sul server MDaemon. Al posto degli allegati effettivi, MDaemon inserisce collegamenti URL che l'utente può selezionare per scaricare gli allegati dal server. Ciò consente un risparmio in termini di larghezza di banda e di memoria, in particolare per quanto riguarda i client e i dispositivi mobili. In MDaemon 11.0, la funzione Collegamento allegati è stata completamente rivista per renderne l'utilizzo più semplice e sicuro. Innanzitutto, la finestra di dialogo Collegamento allegati è stata spostata da Impostazioni account a "Impostazioni » Web, Sincronizzazione e Servizi IM," dal momento che WorldClient svolge un ruolo rilevante per questa funzione. In secondo luogo, la funzione Collegamento allegati prevede due nuove modalità: "*WorldClient gestisce automaticamente Collegamento allegati*" e "*Configura manualmente Collegamento allegati*." Se si seleziona la modalità automatica, che rappresenta l'impostazione predefinita, la funzione utilizza impostazioni interne che l'utente non può modificare. Si tratta della soluzione più semplice e, con WorldClient in esecuzione, non è necessario apportare modifiche alla configurazione. La modalità manuale è necessaria se si desidera collocare gli allegati in un percorso personalizzato.

Alla funzione Collegamento allegati sono state inoltre apportate le modifiche descritte di seguito.

- Tutti gli account configurati per l'utilizzo di Collegamento allegati nelle precedenti versioni ora sono impostati in modo da estrarre gli allegati nella cartella FILES

dell'account. Di conseguenza, può essere necessario riconfigurare manualmente gli account che si desidera utilizzino Collegamento allegati.

- Se si disattiva Collegamento allegati, gli account configurati per utilizzare questa funzione non vengono più reimpostati. Rimangono configurati per l'utilizzo di Collegamento allegati senza, tuttavia, utilizzarlo. Riattivando la funzione, gli account riprendono a utilizzarla immediatamente.
- I collegamenti inseriti da MDaemon nei messaggi non contengono più i percorsi diretti dei file agli allegati. Contengono invece un identificativo univoco (GUID) utilizzato dal server per mappare il file al percorso effettivo. La mappatura dei GUID è memorizzata nel file `AttachmentLinking.dat`.
- La finestra di dialogo Valori predefiniti del nuovo account 377 comprende un'opzione che consente di scegliere le impostazioni predefinite per la gestione degli allegati dei nuovi account.

ADSP DKIM - Supporto RFC 5617 296

Le specifiche ADSP (Author Domain Signing Practices) di DomainKeys Identified Mail (DKIM) sono state definite e rilasciate come RFC 5617. La tecnologia DKIM definisce un framework di autenticazione a livello di dominio della posta elettronica che consente la verifica dell'origine e del contenuto dei messaggi. Le specifiche ADSP offrono un meccanismo di integrazione per la valutazione dei messaggi privi della firma DKIM per il dominio utilizzato nell'indirizzo dell'autore (intestazione DA:). Le specifiche ADSP definiscono un record in grado di indicare se un dominio firma la posta in uscita, nonché le modalità di accesso al record da parte degli altri host.

MDaemon è stato aggiornato in modo da supportare la versione finale di tale specifica. Non è necessario apportare alcuna modifica ai record DKIM o ADSP esistenti. Questo risultato rappresenta la conclusione di più di quattro anni di impegno dell'IETF. Alt-N Technologies consiglia di utilizzare quanto più possibile questo protocollo avvalendosi delle funzioni offerte da MDaemon. È possibile pubblicare il proprio record ADSP sul server DNS, in modo che tutti conoscano i criteri adottati per le firme. È possibile attivare e disattivare ADSP mediante un'opzione della schermata Opzioni DKIM 296.

STLS per DomainPOP e MultiPOP 312

I server DomainPOP e MultiPOP di MDaemon ora supportano STLS. È possibile attivare questa impostazione a livello globale con il seguente percorso: Sicurezza » Impostazioni sicurezza » SSL e TLS » MDaemon. Inizialmente si tenta di utilizzare l'estensione STLS, ma se questa non è supportata dall'altra estremità della connessione, viene avviata una connessione normale. Questa funzione rispetta i criteri del file `NoSTARTTLS.DAT` per l'esclusione dei siti che possono causare problemi.

Per ulteriori informazioni, vedere:

Introduzione 12
Aggiornamento a MDaemon 12.0 24
Schermata principale di MDaemon 28

1.3 Assistenza

Opzioni di supporto

L'assistenza rappresenta una componente essenziale dell'interazione complessiva del cliente con Alt-N Technologies. Desiderando offrire al cliente il massimo rendimento dei prodotti per lungo tempo dopo l'acquisto e l'installazione iniziale, il nostro impegno è rivolto a garantire la risoluzione di eventuali problemi per consentire la massima soddisfazione. Per le informazioni relative al servizio clienti, alle opzioni di assistenza tecnica, alle risorse di supporto autonomo e ai prodotti, visitare la pagina dell'assistenza di Alt-N Technologies all'indirizzo: www.altn.com/support/

Beta-test di MDaemon

Alt-N Technologies gestisce team di beta-test per i propri prodotti. Per informazioni su come unirsi ai beta-team di MDaemon, inviare un messaggio all'indirizzo MDaemonBeta@altn.com.

Il beta-team è dedicato a chi desidera ottenere dei programmi Alt-N prima del rilascio ufficiale collaborando al collaudo. Non si tratta di un'alternativa al supporto tecnico. L'assistenza tecnica per MDaemon viene offerta solo con i metodi descritti alla pagina: www.altn.com/support/.

Contatti

Orari
Lun.-ven. 8:30 - 17:30 (fuso orario degli Stati Uniti centrali)
esclusi weekend e festività statunitensi
Servizio clienti o vendite
Numero verde per gli Stati Uniti: 866-601-ALTN (2586)
Chiamate internazionali: 817-601-3222
sales@helpdesk.altn.com

Assistenza tecnica
www.altn.com/support/

Formazione
training@altn.com

Sviluppo aziendale/collaborazioni
alliance@altn.com

Media/Analisti
press@altn.com

Richieste commerciali/rivenditori
Per ulteriori informazioni, consultare la pagina Channel Partner.

Sede centrale

Alt-N Technologies, Ltd.
2550 SW Grapevine Parkway, Suite 150
Grapevine, Texas 76051
Numero verde per gli Stati Uniti: 866-601-ALTN (2586)
Chiamate internazionali: 817-601-3222
Fax: 817-601-3223

Sezione II

2 Aggiornamento a MDaemon 12.0

Di seguito vengono elencate le considerazioni e le note specifiche di cui tenere conto nell'aggiornamento a MDaemon versione 12.0 da una versione precedente.

Versione 12.0.0

- Il sistema operativo Windows 2000 non è più supportato. MDaemon 12.0 richiede i sistemi operativi Windows 2008, 2003, 7, XP o Vista.
- WorldClient dispone di una versione aggiornata dell'editor WYSIWYG CKEditor per la composizione dei messaggi. In assenza di temi personalizzati, è consigliabile rimuovere la directory `MDaemon\WorldClient\HTML\fckeditor\`. Tale directory non viene rimossa dal programma di installazione a causa della personalizzazione del modello.
- La nuova funzione BES BlackBerry [165] di MDaemon potrebbe comportare la duplicazione dei dati se utilizzata in combinazione con altre tecniche di sincronizzazione quali SyncML o l'integrazione con BIS BlackBerry [184]. Per evitare questo inconveniente, prestare attenzione e consultare Attivazione azienda [167].
- Le password devono essere di almeno 4 caratteri. Non è obbligatorio modificare le password esistenti, ma alle successive modifiche verranno richieste password di almeno 4 caratteri.

Versione 11.0.0

- Come credenziali utente per l'accesso, i server POP e IMAP di MDaemon ora richiedono l'indirizzo di posta elettronica completo. Se la configurazione del client di posta elettronica di un utente prevede l'accesso in base al solo nome della casella postale, ad esempio "franco" anziché "franco@esempio.com", non sarà possibile accedere a MDaemon con il client senza modificarne la configurazione impostandola in modo da utilizzare l'indirizzo di posta elettronica completo. Per continuare a consentire gli accessi con la sola indicazione della casella postale, è necessario disabilitare l'opzione "*Autenticazione con indirizzo di posta elettronica completo*" nella schermata Sistema [194] di Preferenze. È consigliabile, tuttavia, che questa opzione sia abilitata e che venga richiesto l'indirizzo di posta elettronica completo.
- Collegamento allegati [154] ha subito una revisione completa con il conseguente ripristino dei valori di configurazione predefiniti. Durante l'aggiornamento alla versione 11.0 di MDaemon, tutti gli account configurati per l'utilizzo di Collegamento allegati vengono impostati in modo da estrarre gli allegati dalla cartella FILES. Può essere necessario, pertanto, riconfigurare manualmente gli account che si desidera utilizzino Collegamento allegati.
- Il file `WorldClient.dll` è stato aggiornato in modo da generare dinamicamente il file `robots.txt` nella directory HTML di WorldClient per esplicitare i file da non indicizzare. Per disabilitare questa funzione, modificare il file `WorldClient.ini` impostando il valore: `ModifyRobotsTxt=No` nella sezione `[WebServer]`. In alternativa, se il file `robots.txt` è di sola lettura, non viene modificato. È inoltre necessario inserire nell'intestazione dei file `Logon.html` personalizzati il seguente meta tag: `<meta name="ROBOTS" content="NOINDEX, FOLLOW">`.

- I temi Globe e Redline di WorldClient sono stati dismessi e non sono più supportati. Durante la prima esecuzione di MDaemon 11.0, le cartelle \Modelli\ e \HTML\ di questi due temi vengono spostate in \WorldClient\Old\. È possibile eliminarle senza problemi se non si desidera gestire questi due temi manualmente.
- *Check a DKIM DNS Record*, disponibile all'indirizzo http://dkimcore.org/tools/dkimrecordcheck.html, è uno strumento che consente di controllare la conformità dell'impostazione DNS di DKIM con le specifiche DKIM pubblicate in RFC 4871. Dato un selettore e un dominio, lo strumento recupera il record della chiave DKIM dal server DNS, lo analizza utilizzando la codifica BNF inclusa nelle specifiche DKIM, quindi esegue un controllo di integrità dei campi. Al termine, il risultato indica se il controllo è stato superato e se l'impostazione DNS di DKIM è conforme alle specifiche o meno. Nota: il sito è in continua trasformazione e non è ospitato o creato da Alt-N Technologies.
- Le opzioni predefinite per i calcoli delle quote sono state reimpostate. Rivedere le impostazioni della schermata Quote416 per assicurarsi che siano quelle desiderate. L'impostazione predefinita per includere le sottocartelle Posta in arrivo nel calcolo delle quote è stata modificata da FALSE in TRUE.
- Come parte della nuova funzione di integrazione Servizi Internet BlackBerry (BIS)184, per l'accesso a MDaemon è necessario che tutte le sessioni IMAP/POP degli utenti BIS utilizzino un indirizzo di posta elettronica completo. Di conseguenza, quando si configurano i dispositivi BlackBerry per la raccolta di posta, è necessario utilizzare come parametro di accesso l'indirizzo di posta elettronica completo, anziché la sola porzione di indirizzo relativa alla casella postale. Questa operazione è necessaria per evitare possibili conflitti e garantire la corretta integrazione degli account. Per alcuni utenti può essere necessario eliminare e ricreare nuovamente il profilo di posta sul proprio dispositivo o, perlomeno, modificare il valore di accesso con l'indirizzo completo.

Versione 10.1.0

- A causa delle importanti modifiche apportate al tema LookOut di WorldClient nel corso delle ultime versioni di MDaemon e dei progressi delle tecnologie e degli standard Web verificatisi dal 2001, il tema LookOut non supporta più Internet Explorer 6. Gli utenti di Internet Explorer 6 che tentino di utilizzare il tema LookOut verranno reindirizzati automaticamente al tema Standard in modo da poter continuare ad accedere alla propria posta elettronica e ad altri dati GroupWare. È consigliabile aggiornare il browser da Internet Explorer 6 a Internet Explorer 8, che offre significativi miglioramenti in termini di sicurezza, qualità e prestazioni.

Versione 10.0.3

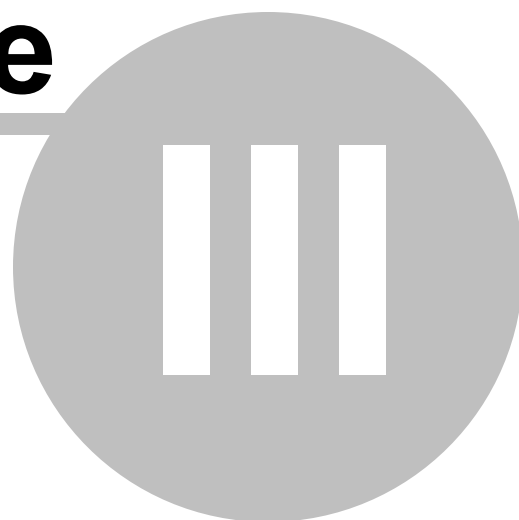
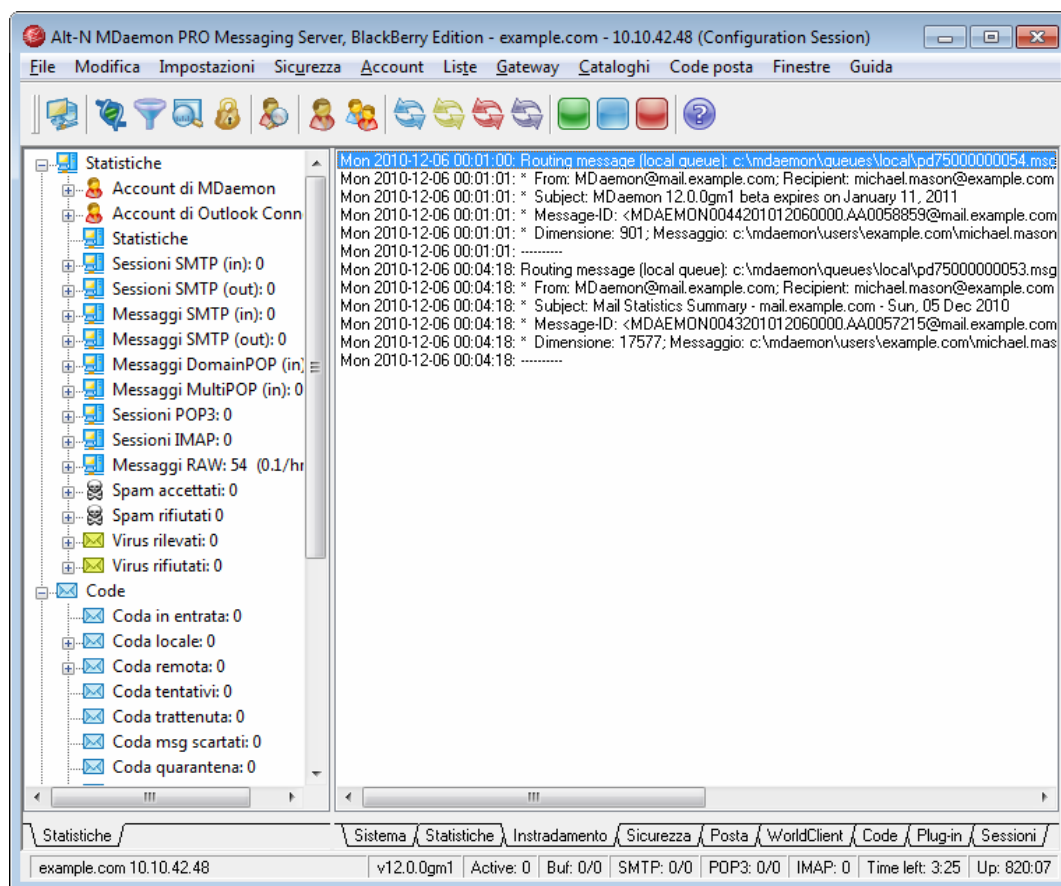
- La funzione Liste nere DNS (DNS-BL) ha subito numerose modifiche relative alla codifica interna. Di conseguenza, è possibile che la funzione DNS-BL267 sia disabilitata dopo l'aggiornamento di MDaemon. Per riabilitarla, utilizzare la schermata Host DNS-BL, situata in: Sicurezza » Spam Filter... » DNS-BL.

Versione 10.0.0

- Questa versione **NON** è compatibile con le versioni precedenti. L'installazione e l'avvio di questa versione determinano modifiche irreversibili a numerosi file di configurazione. **Prima di installare questa versione, eseguire un backup dei file di MDaemon.**
- I file di Pianificazione eventi 156 per la raccolta della posta, gli aggiornamenti AntiVirus 163 e quelli AntiSpam 263 sono stati modificati. Di conseguenza, queste pianificazioni vengono reimpostate tutte sui valori predefiniti di installazione. Verificare le pianificazioni e apportare le modifiche necessarie.
- Il formato dei file dell'indice dei messaggi di WorldClient è stato modificato. Al primo accesso utente, il file verrà aggiornato con il nuovo formato. È prevedibile che il primo accesso risulti rallentato, ma successivamente la velocità dovrebbe essere normale.
- Le impostazioni DNS-BL 267 sono state reimpostate. Controllarle per accertarsi che siano quelle desiderate. Le impostazioni DNS-BL si trovano in Sicurezza » Spam Filter.
- MDaemon Standard non supporta più i gateway di dominio 458. Per le funzioni gateway è necessario eseguire l'aggiornamento a MDaemon PRO.
- MDaemon Standard non prevede più di cinque liste di distribuzione con un massimo di 50 iscritti ciascuna. Per un numero maggiore di liste di distribuzione o per liste più numerose è necessario eseguire l'aggiornamento a MDaemon PRO.
- L'opzione "Registra sempre su schermo" di Registrazione » Opzioni 109 è stata reimpostata sul valore predefinito (disabilitata). È possibile riabilitarla.
- Il file `Signature.dat` non è più utilizzato. Le firme dei singoli account ora vengono memorizzate come file `<email>.sig` nella nuova cartella principale Signatures. MDaemon è in grado di leggere `Signature.dat` e di eseguire la migrazione delle firme di account esistenti nel nuovo formato di file e cartella. È necessario creare nuovamente la firma di dominio predefinita, se utilizzata, mediante la schermata Firme di dominio 74.
- Per un elenco completo delle nuove funzioni, delle modifiche e delle correzioni rispetto alle versioni precedenti di MDaemon, vedere il file `Relnotes.html` nella sottocartella `\Docs\` di MDaemon.

Vedere:

Introduzione 12
Novità di MDaemon 12.0 15
Schermata principale di MDaemon 28

Sezione III

3 Schermata principale di MDaemon

La GUI (interfaccia grafica utente) principale di MDaemon offre importanti informazioni su risorse, statistiche, sessioni attive e posta accodata in attesa di elaborazione. Sono inoltre presenti le opzioni per attivare/disattivare in modo semplice i vari server di MDaemon. I riquadri a schede della GUI forniscono informazioni aggiornate sulle prestazioni del server e sulle connessioni in entrata e in uscita.

Statistiche

Statistiche è il riquadro di sinistra predefinito dell'interfaccia principale di MDaemon. Comprende tre sezioni: Statistiche, Code e Server.

La sezione *Statistiche* include statistiche sul numero di messaggi inviati e ricevuti da MDaemon e sul numero di sessioni POP3 e IMAP iniziate dal momento dell'avvio del server. Questa sezione indica inoltre il numero degli account utente esistenti e quello degli account che è possibile creare. Presenta inoltre due menu di scelta rapida visualizzabili con il pulsante destro del mouse: uno per le voci relative agli account e uno per le voci relative alle statistiche della posta. Il menu di scelta rapida Account fornisce i collegamenti per creare, modificare ed eliminare gli account. Alle voci relative alle statistiche della posta è associato un menu di scelta rapida utilizzabile per azzerare i contatori.

Quando si abilita l'opzione "Azzera contatori nodi principali", vengono resettati tutti i contatori e non solo quelli sui quali si è fatto clic con il pulsante destro del mouse. In Impostazioni » Preferenze » GUI è inoltre disponibile l'opzione "*Mantieni contatori posta nodo principale tra riavvii*." Se questa opzione non è abilitata, quando il server viene avviato i contatori vengono azzerati.

La sezione *Code* include una voce per ogni coda di messaggi e il numero dei messaggi eventualmente contenuti nella coda. È possibile fare clic con il pulsante destro del mouse su ciascuna voce per aprire un menu di scelta rapida contenente una o più delle seguenti opzioni, a seconda della coda selezionata:

Visualizza coda. Consente di passare dal riquadro principale alla scheda Code posta e di visualizzare la coda selezionata. In tal modo, viene visualizzato un elenco di tutti i messaggi presenti nella coda. Facendo clic con il pulsante destro del mouse su uno di questi, è possibile aprire un menu di scelta rapida contenente numerose opzioni analoghe a quelle disponibili in Gestione delle code e delle statistiche, ad esempio Copia, Sposta, Modifica, Lista bianca e così via.

Gestione delle code e delle statistiche. Consente di aprire la Pagina code di Gestione code e statistiche, con la visualizzazione della coda selezionata.

Elabora ora. Consente di "riaccodare" tutti i messaggi contenuti nella coda e di elaborarli normalmente per il recapito. Quando si tenta di elaborare la posta archiviata nella coda trattenuta o in quella dei messaggi scartati, è possibile che si ripetano gli stessi errori a seguito dei quali i messaggi erano stati inseriti in queste code e che i messaggi in questione vengano riposizionati nella stessa coda.

Sospendi/riprendi coda posta. Consente di sospendere temporaneamente l'elaborazione della coda selezionata o di riprenderla se attualmente sospesa.

Rilascia. Rilascia i messaggi della coda trattenuta. MDaemon tenterà di eseguirne la consegna ignorando eventuali errori. I messaggi non torneranno nella coda trattenuta anche se si verificano gli stessi errori che ne hanno causato originariamente l'inclusione.

Riaccoda. Questa funzione è disponibile per la coda trattenuta e svolge lo stesso ruolo descritto in precedenza per *Elabora ora*.

Abilita/disabilita coda. Consente di attivare o disattivare la coda trattenuta. In caso di disattivazione, i messaggi non verranno spostati nella coda trattenuta, a prescindere da eventuali errori.

Nella sezione *Server* è presente una voce associata a ogni server all'interno di MDaemon, che indica lo stato corrente del server, "Attivo" o "Inattivo". Sotto la voce relativa a ogni server, è presente una voce relativa al dominio (se applicabile) e la porta e l'indirizzo IP attualmente in uso per quel server o il dominio. Il menu di scelta rapida fornisce un comando che consente di attivare o disattivare ciascun server. Quando un server è inattivo, la relativa icona diventa rossa.

Monitoraggio e registrazione eventi

Il riquadro predefinito di destra dell'interfaccia principale comprende un gruppo di schede in cui vengono visualizzati lo stato e le azioni correnti dei vari server e delle varie risorse di MDaemon, costantemente aggiornate per riflettere le condizioni effettive del server. Ogni sessione attiva e ogni azione del server vengono registrate nella scheda appropriata al termine delle azioni. Se si è scelto di registrare tale attività, le informazioni visualizzate in queste schede si riflettono nei file di registro conservati nella directory dei registri.

Nel riquadro principale della GUI di MDaemon sono incluse le schede seguenti:

Sistema. All'avvio del programma, in questa scheda viene visualizza la registrazione del processo di inizializzazione che segnala eventuali problemi relativi alla configurazione o allo stato di MDaemon. Sono inoltre mostrate altre attività, ad esempio l'avvio o l'arresto dei vari server di MDaemon.

Statistiche. In questa scheda viene visualizzato il report statistiche del server che corrisponde alle informazioni contenute nei diversi contatori relativi ai nodi principali della scheda Statistiche nel riquadro relativo alle statistiche e agli strumenti. Per modificare il tipo o la dimensione dei caratteri utilizzati per il report, modificare le seguenti impostazioni del file MDaemon.ini:

```
[ReportWindow]
DefFontFace=Courier New
DefFontHeigh=15
DefFontWidth=7
```

Ogni notte a mezzanotte, una copia del report verrà inviata via posta elettronica al Postmaster e a tutti gli indirizzi elencati nella schermata Destinatari229 di Filtro contenuti. Si tratta dello stesso report generato con l'utilizzo del comando e-mail "Status" descritto nella sezione Controllo remoto del server via e-mail. Se non si desidera che il report venga inviato, disabilitare l'opzione "*Invia report statistiche al postmaster a mezzanotte*" della schermata Opzioni varie202 di Preferenze.

Instradamento. Consente di visualizzare informazioni relative all'instradamento (To, From, Message-ID e così via) di ciascun messaggio analizzato da MDaemon.

Sicurezza. Facendo clic su questa scheda, verranno visualizzate le altre schede correlate alla sicurezza.

Filtro contenuti. In questa scheda vengono elencate le operazioni di Filtro contenuti212. Quando un messaggio viene analizzato per la presenza di virus o risponde ai criteri di Filtro contenuti, le informazioni e le operazioni compiute in relazione al messaggio vengono registrate in questa scheda.

AntiVirus. In questa scheda vengono elencate tutte le operazioni eseguite da SecurityPlus per MDaemon211, se installato. Quando un messaggio viene esaminato per rilevare l'eventuale presenza di virus, tutte le informazioni relative al messaggio e le operazioni eseguite al riguardo vengono registrate in questa scheda.

AntiSpam. Vengono visualizzate tutte le operazioni di Spam Filter243 e le attività di prevenzione.

MDSpamD. Vengono visualizzate tutte le attività di MDaemon Spam Daemon 253.

SPF/ID mittente. Vengono visualizzate tutte le attività relative a SPF (Sender Policy Framework) e a ID mittente 285.

DK/DKIM. Vengono elencate tutte le attività relative a DomainKeys e a DomainKeys Identified Mail 287.

Certificazione VBR. Questa scheda consente di visualizzare le attività di Certificazione VBR 298.

Vaglio. In questa scheda vengono visualizzate le attività relative al tarpitting 329 e al vaglio dinamico 309.

Posta. Facendo clic su questa scheda, verranno visualizzate altre schede correlate al di sopra di essa.

SMTP (entrata). In questa scheda vengono visualizzate tutte le attività della sessione in entrata che utilizza il protocollo SMTP.

SMTP (uscita). In questa scheda vengono visualizzate tutte le attività della sessione in uscita che utilizza il protocollo SMPT.

IMAP. In questa scheda vengono registrate le sessioni di posta che utilizzano il protocollo IMAP.

POP3. In questa scheda vengono registrate le attività degli utenti che raccolgono la posta elettronica da MDaemon mediante il protocollo POP3.

MultiPOP. In questa scheda vengono visualizzate le attività di raccolta della posta MultiPOP di MDaemon.

DomainPOP. In questa scheda vengono visualizzate le attività DomainPOP di MDaemon.

LDAP. Vengono visualizzate le attività del server LDAP.

Minger. Mostra l'attività del server Minger 418.

RAW. In questa scheda vengono registrate le attività di posta RAW o generata dal sistema.

Outlook Connector. Vengono visualizzate le attività di Outlook Connector.

BES. vengono visualizzate le attività relative all'integrazione di MDaemon con BlackBerry Enterprise Server 165.

BIS. Vengono visualizzate le attività relative all'integrazione di MDaemon con BlackBerry Internet Service 186.

WorldClient

WorldClient. Vengono visualizzate le attività della sessione di WorldClient.

SyncML. Questa scheda riflette i dati contenuti nel file registro di SyncML.

Code. Questa scheda consente di accedere a un altro insieme di schede al di sopra della scheda stessa, in cui ogni scheda corrisponde a una coda di messaggi, ad esempio: locale, remota, trattenuta, quarantena, bayesiana e così via.

Plug-in. Vengono visualizzate tutte le attività correlate ai plug-in di MDaemon.

Sessioni. Facendo clic su questa scheda, vengono visualizzate altre schede al di sopra di essa, in ciascuna delle quali viene visualizzata una voce per ogni connessione a MDaemon attiva. La voce indica se la connessione è di tipo SMTP in entrata o SMTP in uscita, POP in entrata o POP in uscita, IMAP, WorldClient oppure di altro tipo e riporta informazioni relative a ciascuna sessione attiva. Facendo doppio clic su una sessione attiva, viene visualizzata la finestra Sessione 35, con la trascrizione dello stato di avanzamento della sessione SMTP.

Le informazioni visualizzate in queste schede non hanno alcun effetto sulla quantità di dati effettivamente memorizzata nei file registro. MDaemon è particolarmente flessibile per la quantità e il tipo di informazioni registrate in tali file. Per ulteriori informazioni sulle opzioni di registrazione, vedere la finestra di dialogo relativa alle opzioni di registrazione 103.

Menu di scelta rapida della finestra di monitoraggio degli eventi

Facendo clic con il pulsante destro del mouse in una qualsiasi delle schede del riquadro Monitoraggio eventi, si apre un menu di scelta rapida. Questo menu include diverse opzioni che consentono di selezionare, di copiare, di eliminare o di salvare i contenuti di una determinata scheda. L'opzione *Stampa/Copia* del menu apre in Blocco note il testo selezionato consentendo così di stampare i dati o salvarli in un file. L'opzione *Elimina* consente di eliminare il testo selezionato e la voce di menu *Posta per supporto* consente di aprire il testo selezionato in una finestra che è possibile utilizzare per inviare un messaggio al supporto tecnico. L'opzione *Ricerca* consente di aprire una finestra in cui è possibile specificare una parola o una frase da cercare nei file di registro. MDaemon eseguirà la ricerca della stringa di testo in tutti i file di registro. Successivamente, tutte le trascrizioni delle sessioni contenenti tale stringa saranno riunite in un singolo file e aperte in Blocco note per una verifica. Questa funzione si rivela utile, ad esempio, nel caso di una ricerca di una specifica intestazione Message-ID, fornendo la selezione, ricavata da tutti i file di registro, di tutte le trascrizioni delle sessioni che contengono tale Message-ID.

Il layout dell'interfaccia grafica di MDaemon non si limita alle posizioni predefinite descritte in precedenza. Le posizioni possono essere modificate facendo clic su Finestre » Cambia riquadri nella barra dei menu.

Vista Registro globale

Nel menu Finestre della barra dei menu di MDaemon è presente l'opzione Vista Registro globale. Facendo clic su questa opzione, alla GUI verrà aggiunta una finestra in cui sono visualizzate congiuntamente le informazioni appartenenti a una o più schede del riquadro principale. Le opzioni della schermata Registro composito 106 della finestra di dialogo Registrazione consentono di indicare le informazioni che verranno visualizzate in questa finestra.

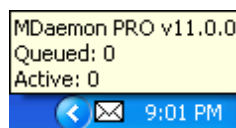
Per ulteriori informazioni, vedere:

Finestra Sessione 35
Icona della barra delle applicazioni 33
Menu di scelta rapida 34
Registro composito 106

3.4 Icona della barra delle applicazioni

Quando il server MDaemon è in esecuzione, nella barra delle applicazioni è visibile un'icona. Si tratta di un'icona dinamica che, oltre a indicare se il sistema è in esecuzione, cambia colore a seconda dello stato corrente del server. Di seguito è riportato un elenco dei vari aspetti possibili dell'icona.

✉	Funzionamento regolare. Assenza di posta nelle code locali e remote.
✉ (blu)	Funzionamento regolare. Presenza di posta nelle code locali o remote.
✉ (giallo)	Spazio su disco inferiore alla soglia (vedere Impostazioni » Preferenze » Disco 197).
✉ (rosso)	Rete inattiva, connessione non riuscita o disco pieno.
Icona lampeggiante	È disponibile una versione di MDaemon più recente.

La descrizione comandi dell'icona fornisce ulteriori informazioni sul server. Posizionare il puntatore sopra l'icona per visualizzare la descrizione comandi che consente di visualizzare il numero di messaggi attualmente in coda e il numero di sessioni attive.

Menu di scelta rapida

Per aprire il menu di scelta rapida (o menu contestuale), fare clic con il pulsante destro del mouse sull'icona MDaemon nella barra delle applicazioni. Questo menu permette di accedere rapidamente a tutti i menu e a tutte le funzionalità di MDaemon, senza dover aprire l'interfaccia utente principale.

Per ulteriori informazioni su MDaemon o su Alt-N Technologies, fare clic sulle opzioni "Info su Alt-N..." nella sezione superiore del menu di scelta rapida.

Nella sezione successiva, facendo clic su " Controlla aggiornamenti MDaemon" è possibile verificare la disponibilità di versioni più recenti di MDaemon.

La terza sezione consente di accedere ai seguenti menu di MDaemon: Impostazioni, Sicurezza, Account, Liste, Gateway, Cataloghi e Code posta. Ognuno di questi menu è identico all'omonimo menu presente nella barra dei menu dell'interfaccia principale.

Nella quarta sezione sono disponibili le opzioni che consentono di accedere alle finestre Account Manager e Gestione code e statistiche, nonché un'opzione che permette di elaborare tutte le code di posta di MDaemon.

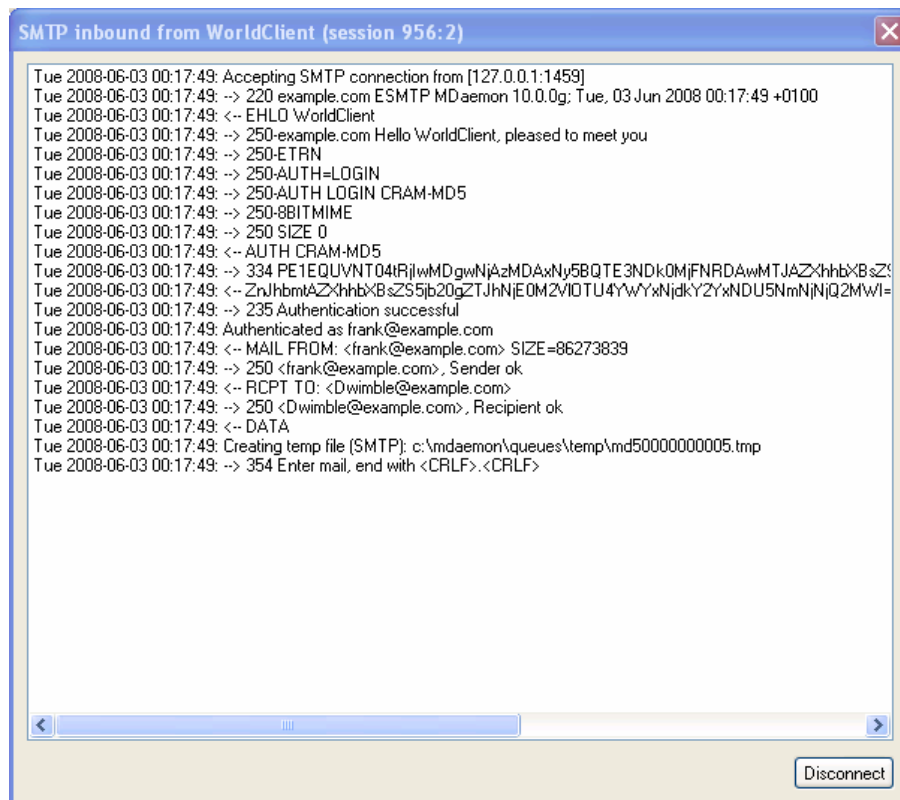
Nella sezione successiva sono disponibili i comandi che consentono di bloccare e sbloccare l'interfaccia di MDaemon (vedere il successivo argomento "Blocco/sblocco dell'interfaccia principale di MDaemon"), seguiti dal comando Apri MDaemon, utilizzato per aprire o ripristinare l'interfaccia di MDaemon se quest'ultima è ridotta a icona nella barra delle applicazioni.

L'ultima opzione è "Chiudi MDaemon" che viene utilizzata per uscire da MDaemon o per chiudere il relativo servizio di sistema. Le impostazioni del servizio non vengono modificate; l'unica azione eseguita è l'arresto del servizio MDaemon.

Blocco/sblocco dell'interfaccia principale di MDaemon

Per bloccare l'interfaccia utente ridurre a icona MDaemon, fare clic sulla voce di menu "Blocca server" e inserire una password nella finestra di dialogo visualizzata. Dopo aver confermato la password inserendola una seconda volta, l'interfaccia utente di MDaemon sarà bloccata. Non è possibile aprirla o visualizzarla, ma MDaemon continua a funzionare normalmente. È comunque possibile utilizzare l'opzione "Elabora tutte le code" per elaborare manualmente le code di posta. Per sbloccare MDaemon, fare doppio clic sull'icona che si trova sulla barra delle applicazioni e aprire la finestra di dialogo "Sblocca MDaemon". In alternativa, fare clic sull'icona con il pulsante destro del mouse e scegliere "Sblocca server", quindi inserire la password creata per il blocco dell'interfaccia.

3.5 Finestra Sessione

Quando si fa doppio clic su una sessione attiva di una delle schede Sessioni 30 della GUI principale, viene aperta la relativa finestra. In questa finestra viene visualizzata la trascrizione SMTP della sessione in corso. Per interrompere e disconnettere la sessione in corso, fare clic su Disconnetti nella finestra.

3.6 Flusso di lavoro SMTP di MDaemon

Quando viene stabilita una connessione SMTP, MDaemon effettua una complessa serie di passi elaborativi per determinare se accettare il messaggio e come operare in caso affermativo. Nello schema seguente viene fornita una rappresentazione grafica di questo flusso di lavoro per i messaggi SMTP in ingresso.

l'effettiva esecuzione di questi passi dipende dalla specifica configurazione in uso. Se nella configurazione una particolare funzione è disabilitata, alcuni passaggi potrebbero essere ignorati.

Inbound SMTP
SMTP Server Starts
Update Active Counter
Make sure this session does not exceed the max inbound limit
Check connection to user database
Tarpit
IP Screen
SSL Handshake
Reverse Lookup on IP
Receive EHLO
Host Screening
Reverse Lookup on EHLO
SMTP AUTH
Mail Command Given
ESMTP Size Check
IP Shielding
Reverse Lookup on Mail Command
If to a local user check for a valid local acocunt
POP Before SMTP
If AUTH match sender info
RCPT command given
Tarpit
Check Aliases
Check Address book
Auto Gateway Creation Check
POP before SMTP
Suppression File
IP Shielding
Is AUTH required and given?
Relay Check
Gateway Quota
User Quota
If TO list is sender allowed?
LDAP Gateway Check
Grey Listing
Spam Blocker RBL
DATA command Given
RFC compliance check
Spam Blocker check received headers
Domainkeys
DKIM
SPF
Plugins
Inline Virus Scan
Inline spam filter
User Quota check
At this point the SMTP server is done. The MTA takes over from here.
If To List Crack Message
Local/Remote Queue
Archive
Create new Received header and add DK/DKIM/ SPF headers
Add List Header/ Footer
Header Translation
AntiVirus
Outbreak Protection
Spam Filter
Content Filter
Final Delivery if Local

Sezione IV

4 Menu Impostazioni

4.1 Dominio predefinito/server

4.1.1 Dominio predefinito/server

La sezione Dominio predefinito/server è raggiungibile mediante la selezione di menu Impostazioni » Dominio predefinito/server e consente di configurare il dominio predefinito unitamente ad altre opzioni del server. È possibile configurare un solo dominio predefinito, ma MDaemon è in grado di gestire la posta dei domini aggiuntivi 114 (solo con MDaemon PRO) e dei gateway di dominio 458 desiderati.

La sezione Dominio predefinito include le seguenti finestre di dialogo, necessarie per la configurazione di MDaemon.

Dominio 41
Questa schermata contiene il nome e l'indirizzo IP del dominio predefinito.

Consegna 42
In questa finestra è possibile specificare le opzioni per ripartire il carico di gestione della posta di MDaemon da recapitare a un ISP, un host gateway o un altro server per la consegna all'utente.

Server 46
Questa schermata consente di configurare numerose opzioni relative ai server e ai protocolli e-mail. Esistono, ad esempio, delle opzioni che consentono di scegliere se il server SMTP di MDaemon accetterà comandi VRFY, EXPN, APOP, CRAM-MD5 e altri. È inoltre possibile indicare un limite per la dimensione dei messaggi, limitare il numero delle istruzioni RCPT consentite durante la sessione SMTP e configurare numerose altre opzioni.

Porte 49
Questa schermata è relativa alle porte monitorate e utilizzate da MDaemon per la consegna della posta SMTP e POP. È inoltre possibile indicare la porta da assegnare a MDaemon per il monitoraggio degli eventi IMAP, la porta UDP utilizzata per interrogare i server DNS e numerose altre impostazioni relative alle porte. In genere, non è necessario modificare le impostazioni predefinite. Tuttavia, è opportuno conoscere il meccanismo di configurazione di queste porte per un'eventuale integrazione del server MDaemon con altri componenti o server in uso nella rete.

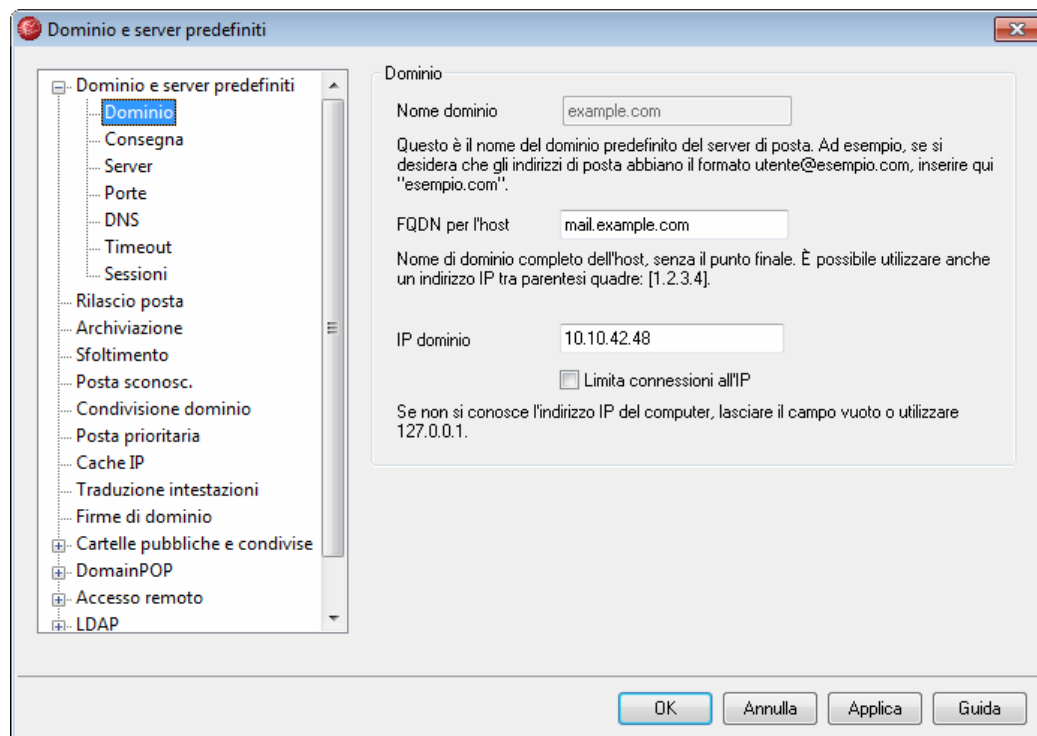
DNS 51
Questa finestra consente di specificare gli indirizzi IP del server DNS principale e di backup. Include numerose altre opzioni per la gestione dei record MX da parte di MDaemon.

Timeout 56
In questa area sono riportati alcuni intervalli temporali che regolano le connessioni agli host remoti, nonché i tempi di attesa per lo scambio di protocolli, per le risposte dai server DNS e così via. Include inoltre il valore *N. max hop messaggi*, utilizzato per impedire che i messaggi vengano coinvolti in un loop di consegna della posta.

Sessioni 56
Consente di definire il numero massimo di thread di sessioni simultanee utilizzate da MDaemon per inviare e ricevere la posta SMTP, POP e IMAP, nonché il numero di messaggi che MDaemon tenterà di inviare/ricevere contemporaneamente. È anche possibile impostare un valore limite sul numero di messaggi SMTP in uscita accodati per ogni thread di sessione.

Vedere:

Hosting di domini multipli 113
Dominio aggiuntivo 114
Domini gateway 458
Raccolta posta DomainPOP 82

4.1.1.1 Dominio

Dominio

Nome dominio
Immettere il nome del dominio predefinito. Si tratta del nome del dominio predefinito che viene utilizzato quando si crea un nuovo account, utilizzato anche per gli account WorldClient creati automaticamente dalle funzioni di integrazione tra MDaemon e WorldClient. Normalmente, il valore inserito in questo campo corrisponde al nome del dominio Internet registrato che un server DNS trasforma nell'indirizzo IP del sistema locale su cui è in esecuzione il server oppure in un alias qualificato di

quel nome.

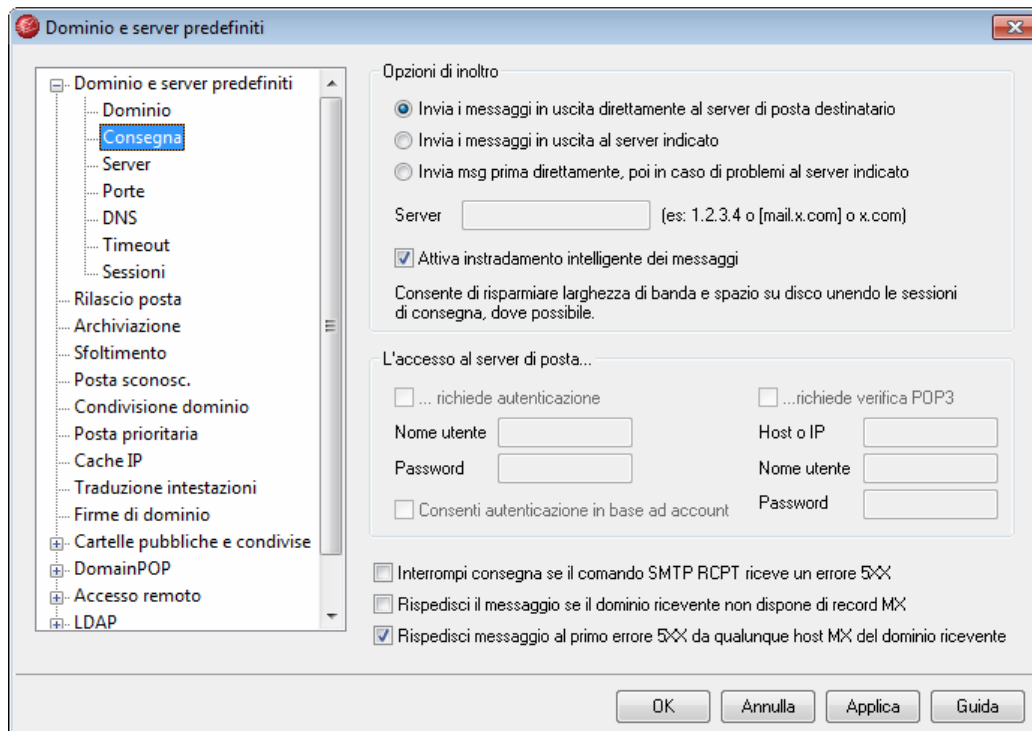
In alternativa, è possibile utilizzare come nome del dominio predefinito un nome a uso interno o un nome di dominio privato e non valido, ad esempio "`company.mail`". Affinché la posta possa essere distribuita correttamente in questo tipo di configurazione del server, può essere necessario utilizzare la funzione Traduzione intestazione 72 e/o Sostituzione nomi di dominio 88.

FQDN per l'host
Questo valore rappresenta il nome di dominio completo (FQDN, Fully Qualified Domain Name) utilizzato nell'istruzione SMTP HELO/EHLO al momento di inviare la posta. Nella maggior parte dei casi coincide con il nome del dominio predefinito. È consentita anche una sintassi letterale IP, ad esempio "`[1.2.3.4]`".

IP dominio
Indica l'indirizzo IP del dominio predefinito.

Limita connessioni all'IP
Selezionando questa opzione, MDaemon limita le connessioni del dominio predefinito al solo indirizzo IP specificato nella casella di testo *IP dominio*. In genere, questo comando è necessario solo per l'hosting di domini multipli.

Per ulteriori informazioni su questo tipo di configurazione, vedere: **Hosting di domini multipli** 113

4.1.1.2 Consegna

Opzioni di consegna

Invia tutte le e-mail in uscita direttamente al server di posta del destinatario.
Se si seleziona questa opzione, MDaemon tenterà di inviare direttamente tutta la posta, anziché inoltrarla a un altro host. MDaemon colloca tutti i messaggi non recapitati nel sistema di gestione dei tentativi e prosegue con le operazioni di invio, in base ai parametri e agli intervalli di tempo impostati nella schermata Coda tentativi484 della finestra di dialogo Code posta. Per accedere alla schermata dalla barra dei menu di MDaemon, fare clic su "Code posta » Code posta... » Coda tentativi".

Invia i messaggi in uscita al server indicato
Questa opzione consente di eseguire lo spool delle e-mail in uscita, indipendentemente dal dominio di destinazione, verso un host o un server per la consegna instradata. Se questa opzione è abilitata, tutte le e-mail in uscita vengono inviate all'host o al dominio specificato nell'opzione *Server*. Questa funzione è utile soprattutto quando il traffico è più intenso e la consegna diretta della posta può determinare un carico eccessivo per le risorse del server. Se non è possibile recapitare un messaggio al server specificato, MDaemon lo colloca nel sistema di gestione dei tentativi e prosegue con le operazioni di invio, in base ai parametri e agli intervalli di tempo impostati nella schermata Coda tentativi484 della finestra di dialogo Code posta.

Invia msg prima direttamente, poi in caso di problemi al server indicato
Questa opzione consente di eseguire lo spool della posta elettronica in uscita non recapitata al dominio o all'host specificato nell'opzione *Server*. Con posta non recapitata si indicano i messaggi indirizzati agli host che potrebbero essere stati inoltrati a un indirizzo IP non reale (ad esempio, un gateway non registrato su una rete remota) oppure i messaggi indirizzati a un host che è stato identificato correttamente ma a cui non è stato possibile collegarsi direttamente o che rifiuta la connessione diretta. Se questa opzione è selezionata, anziché restituire la posta ai rispettivi mittenti, MDaemon inoltra il messaggio a un MTA (Message Transfer Agent, Agente di trasferimento di messaggi) più potente. In alcuni casi, il sistema di posta adottato dall'ISP fa ricorso a metodi di ridistribuzione della posta non accessibili direttamente dal server locale. Se non è possibile recapitare un messaggio al server specificato, MDaemon lo colloca nel sistema di gestione dei tentativi e prosegue con le operazioni di invio, in base ai parametri e agli intervalli di tempo impostati nella schermata Coda tentativi484 della finestra di dialogo Code posta. Per ogni successivo tentativo di consegna, MDaemon tenterà innanzitutto di recapitare il messaggio direttamente al destinatario e, quindi, al dominio o all'host specificato.

Server
Inserire il nome o l'indirizzo IP dell'ISP o dell'hostdi posta. Il valore corrisponde generalmente al server SMTP dell'ISP.

Non inserire in questa casella di testo il dominio predefinito o gli indirizzi IP di MDaemon. A questa voce deve corrispondere un ISP o un altro server di posta in grado di inoltrare la posta.

Attiva instradamento intelligente dei messaggi
Per impostazione predefinita, quando è possibile MDaemon conserva una sola copia di ogni messaggio inviato a più destinatari e utilizza più comandi RCPT per consegnare il messaggio. Ciò consente di risparmiare spazio su disco e larghezza di banda. Se selezionata, ad esempio, questa opzione è attiva ogni volta che un singolo messaggio viene indirizzato a più destinatari dello stesso dominio. Se inoltre si utilizza l'opzione di consegna "*Invia i messaggi in uscita al server indicato*", che consente di inviare la posta in uscita al solo host indicato, MDaemon archivia una singola copia di ogni messaggio e utilizza più comandi RCPT anche se i destinatari appartengono a domini diversi.

L'accesso al server di posta...

Come misura di sicurezza aggiuntiva, alcuni smart host o ISP richiedono ai propri utenti di autenticarsi mediante le credenziali di accesso o di controllare la casella postale POP prima di poter accedere ai server e inviare la posta. Se necessario per l'ISP o l'host di posta, utilizzare questa opzione per specificare le credenziali POP o di login.

...richiede autenticazione
Selezionare questa casella di controllo se l'ISP o l'host al quale si inviano i messaggi richiede l'autenticazione. Inserire le credenziali di accesso nelle caselle di testo sottostanti. Le credenziali verranno utilizzate per tutt i messaggi SMTP in uscita inviati al server specificato in precedenza. Qualora si scelga di utilizzare l'opzione *Consenti autenticazione in base ad account*, MDaemon eseguirà l'autenticazione all'host per ogni messaggio utilizzando l'impostazione *Password/utente host intelligente facoltativa* dell'account mittente, indicata nella schermata Dettagli account 343 di Account Editor.

Nome utente
Immettere il nome utente o di login.

Password
Utilizzare questa opzione per specificare la password di accesso all'ISP o all'host di posta.

...richiede verifica POP3
Se l'ISP o l'host della posta richiedono una verifica POP3 prima di accettare i messaggi inviati dall'utente, selezionare questa casella di controllo e inserire le credenziali necessarie nelle caselle di testo sottostanti.

Host o IP
Immettere il nome dell'host o l'indirizzo IP a cui connettersi.

Nome utente
Si tratta dell'ID utente o del nome dell'account POP.

Password
È la password dell'account POP.

Consenti autenticazione in base ad account
Selezionare questa casella di controllo se si desidera utilizzare l'autenticazione in base all'account per i messaggi SMTP in uscita inviati al *server* specificato in precedenza. Anziché utilizzare le credenziali *Nome utente* e *Password* indicate, per l'autenticazione verrà utilizzata l'impostazione *Utente/password host intelligente facoltativa* dei singoli account specificata nella schermata Dettagli account[343] di Account Editor. Se, tuttavia, per un account non è stata specificata alcuna impostazione *Utente/password host intelligente facoltativa*, verranno utilizzate le credenziali indicate precedentemente.

Per configurare l'*autenticazione in base ad account* in moda che venga utilizzata la *Password e-mail* di un account anziché la *Password host intelligente*, modificare la seguente chiave del file `MDaemon.ini`:

```
[AUTH]
ISPAUTHUsePasswords=Yes (il valore predefinito è No)
```

Se si abilita l'opzione `ISPAUTHUsePasswords=Yes`, con l'andar del tempo tutte la password e-mail locali verranno comunicate all'host intelligente e ciò potrebbe rappresentare un rischio per la sicurezza perché queste informazioni riservate vengono comunicate a un altro server. Non è consigliabile utilizzare questa opzione a meno che l'host intelligente utilizzato non sia di assoluta fiducia e solo se questa operazione è assolutamente necessaria. Tenere presente, inoltre, che se si utilizza questa opzione e si consente agli utenti di modificare la propria *Password e-mail* utilizzando WebAdmin o un altro metodo, la modifica della *Password e-mail* implica anche la modifica della *Password host intelligente*. Di conseguenza, l'autenticazione di un account potrebbe non riuscire qualora la *Password e-mail* venga cambiata localmente, ma la corrispondente *Password host intelligente* non venga modificata nell'host intelligente stesso.

Interrompi consegna se il comando SMTP RCPT riceve un errore 5XX
Se si abilita questa opzione, MDaemon interromperà i tentativi di consegna di un messaggio quando, in risposta a un comando RCPT SMTP, riceverà un errore irreversibile 5xx. L'opzione è disabilitata per impostazione predefinita.

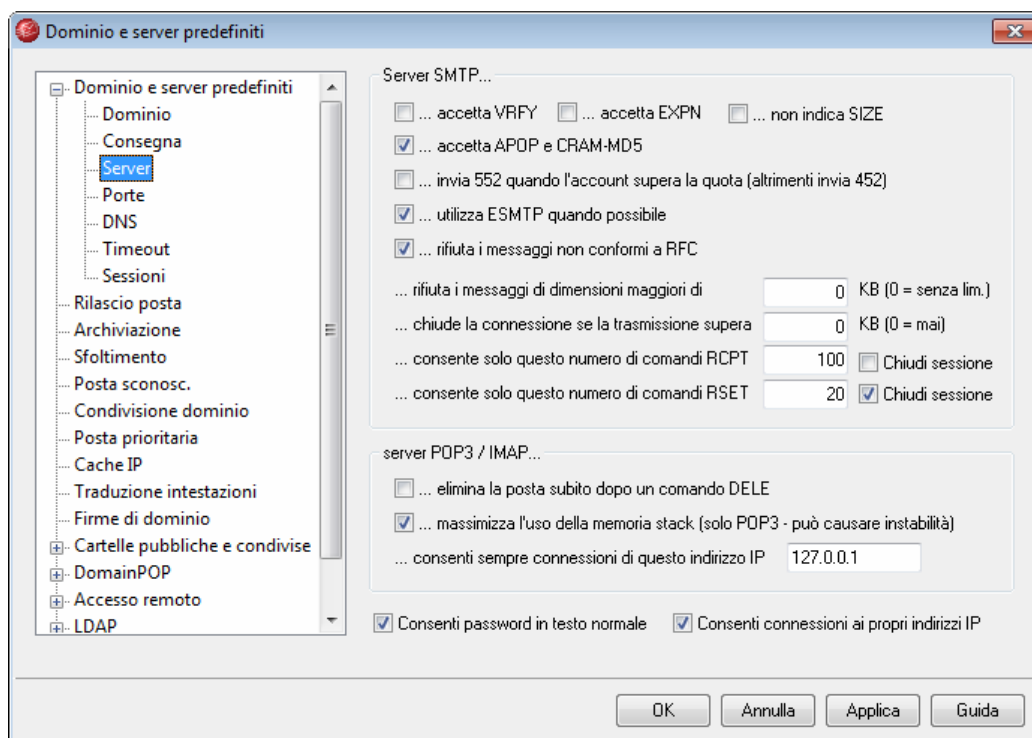
Rispedisci messaggio se dominio ricevente non ha record MX
In genere, quando MDaemon verifica i record DNS del dominio ricevente, cerca i record MX e, in mancanza di questi, un record A. Se non ne trova alcun tipo di record, rispedisce il messaggio al mittente come non recapitato. Se si desidera che MDaemon rispedisca immediatamente il messaggio al mittente in assenza di record MX, anziché cercare anche il record A, selezionare questa opzione. L'opzione è disabilitata per impostazione predefinita.

Rispedisci messaggio al primo errore 5XX da qualunque host MX del dominio ricevente
Se questa casella di controllo è abilitata, MDaemon restituisce o rispedisce il messaggio quando riceve un errore 5xx da un host MX. Di conseguenza, non tenta di

consegnare il messaggio ai successivi host MX eventualmente indicati per il dominio del ricevente. Se questa opzione è disabilitata, MDaemon evita di rispedire il messaggio fino a quando almeno uno degli host MX restituisce un codice di errore 4xx. L'opzione è abilitata per impostazione predefinita.

Per ulteriori informazioni, vedere:

Coda tentativi 484

4.1.1.3 Server

Il server SMTP...

...consente VRFY
Selezionare questa opzione per rispondere ai comandi VRFY di SMTP. Questa opzione viene utilizzata talvolta dai server che utilizzano una funzione di inoltro della chiamata o di richiamata SMTP per confermare la validità degli indirizzi e-mail del server. È disabilitata per impostazione predefinita.

...consente EXPN
Selezionare questa casella di controllo se si desidera che MDaemon accetti i comandi EXPN.

...non pubblica SIZE
Selezionare questa casella di controllo per nascondere il parametro del comando SIZE.

...consente APOP e CRAM-MD5

Per impostazione predefinita, i server di MDaemon, ad esempio i server POP, IMAP e così via, accettano i metodi di autenticazione APOP e CRAM-MD5. Questi metodi offrono una sicurezza aggiuntiva, poiché consentono l'autenticazione degli utenti senza l'invio di password in testo non crittografato. Se non si desidera consentire l'autenticazione APOP o CRAM-MD5, deselezionare questa casella di controllo.

...invia il codice 552 (anziché 452) per superamento quota account

Questa opzione determina una risposta 552 ("Azione richiesta interrotta: spazio dedicato superato") quando viene tentata la consegna a un destinatario il cui account supera la quota364 stabilita. Normalmente, la risposta è 452 ("Azione richiesta respinta: spazio su sistema insufficiente").

...utilizza ESMTP ove possibile

Quando si abilita questa opzione, MDaemon supporta i comandi SMTP estesi. Per impostazione predefinita, questa opzione è abilitata.

...rifiuta i messaggi non conformi a RFC

Questa opzione consente di respingere, durante l'elaborazione SMTP, i messaggi non conformi agli standard Internet RFC. Per superare il test di conformità, è necessario che il messaggio:

1. abbia dimensioni superiori a 32 byte (dimensione minima per includere tutte le parti necessarie);
2. disponga dell'intestazione DATE;
3. disponga dell'intestazione FROM o SENDER;
4. non abbia più intestazioni FROM;
5. non abbia più intestazioni SUBJECT, anche se tale intestazione non è obbligatoria.

I messaggi che utilizzano sessioni autenticate o che provengono da domini accreditati o da indirizzi IP sono esenti da tali requisiti.

...rifiuta i messaggi superiori a [xx] KB (0=senza lim.)

Questo campo consente di impedire che MDaemon accetti o elabori la posta SMTP consegnata che supera una determinata dimensione. Se questa opzione è abilitata, MDaemon tenta di utilizzare il comando ESMTP SIZE specificato in RFC-1870. Se il programma di invio supporta questa estensione SMTP, MDaemon determina la dimensione del messaggio prima della consegna effettiva e, in caso, lo rifiuta immediatamente. Se il programma di invio non supporta questa estensione SMTP, MDaemon deve avviare l'accettazione del messaggio, monitorarne regolarmente la dimensione durante il trasferimento e rifiutarlo solo al termine della transazione. Specificare "0" in questa opzione se non si desidera impostare alcun limite di dimensione.

...chiude connessione se trasm. dati supera [xx] KB (0=mai)

Se i dati trasmessi durante una connessione con MDaemon superano questa soglia, MDaemon chiude la connessione.

...consenti solo questi comandi RCPT [xx] (RFC = 100)
Questa opzione consente di limitare il numero di comandi RCPT che possono essere inviati per messaggio.

Chiudi sessione
Questa casella consente di chiudere la sessione appena raggiunto il numero massimo di comandi RCPT consentito.

...consenti solo questo numero di comandi RSET [xx]
Questa opzione consente di impostare il numero massimo di comandi RSET consentito per una sessione SMTP (il valore predefinito è 20).

Chiudi sessione
Questa casella consente di chiudere la sessione appena raggiunto il numero massimo di comandi RSET consentito.

Server POP3 / IMAP

...elimina posta immediatamente al comando DELE
Selezionare questa opzione per consentire a MDaemon di eliminare immediatamente i messaggi che gli utenti hanno ritirato, anche se la sessione POP non è stata chiusa correttamente.

...massimizza l'uso della memoria stack (solo POP3 - può causare instabilità)
Questa opzione consente di aumentare al massimo l'uso di memoria stack di MDaemon per evitare i problemi che potrebbero verificarsi quando gli account POP attivi contengono diverse migliaia di messaggi. Disabilitando questa opzione, il server POP diventa più conservativo, ma quando il server POP è molto carico potrebbero aumentare i tempi di risposta dell'interfaccia.

...consenti sempre connessioni di questo indirizzo IP
I server POP e IMAP accettano sempre le connessioni dall'indirizzo IP immesso in questo campo, indipendentemente dalle impostazioni relative a Vaglio IP e Scudo IP.

-

Consenti password in testo normale
Con questa opzione si consente a MDaemon di accettare password in chiaro inviate ai server SMTP, IMAP o POP3. Se viene disabilitata, i comandi `POP3 USER`, `POP3 PASS`, `IMAP LOGIN`, `IMAP AUTH LOGIN` e `SMTP AUTH LOGIN` daranno come risultato un errore a meno che la connessione non utilizzi SSL.

Consenti connessioni ai propri indirizzi IP
Abilitando questa opzione, MDaemon è in grado di connettersi con sé stesso.

4.1.1.4 Porte

Porte SMTP/ODMR/MSA (alcune funzionalità richiedono MDaemon PRO)

Porta SMTP in entrata
MDaemon controlla questa porta TCP per rilevare eventuali connessioni in arrivo da client SMTP. Si tratta della porta SMTP principale, che in genere viene lasciata inalterata sul valore predefinito 25.

Porta SMTP in uscita
Questa porta viene utilizzata quando la posta viene inviata ad altri server SMTP.

Porta MSA in entrata
La porta MSA (Message Submission Agent) può essere utilizzata dagli utenti in alternativa alla *Porta SMTP in entrata* specificata in precedenza. Se si utilizza questa porta alternativa l'autenticazione è obbligatoria e, di conseguenza, è necessario configurare correttamente i propri client di posta al fine di garantire l'autenticazione delle connessioni. Inoltre, poiché alcuni ISP bloccano la porta 25, gli utenti remoti hanno la possibilità di eludere tale restrizione utilizzando la porta MSA. Se non si desidera definire una porta MSA, impostare il valore su "0" per disattivarla.

Le connessioni alla porta MSA sono escluse dalle ricerche PTR e inverse, da Vaglio Host e Vaglio IP, da Scudo IP e dalla funzione di tarpitting. Le connessioni della porta MSA utilizzano ancora la limitazione delle connessioni di attacco in base al dizionario.

Porta ODMR in entrata
MDaemon monitora questa porta per rilevare le connessioni ODMR (On-Demand Mail Relay) in entrata, ad esempio il comando `ATRN` dei gateway di dominio.

Porta SSL SMTP
Si tratta della porta dedicata per le sessioni di posta SMTP che utilizzano una connessione SSL (Secure Sockets Layer). Per ulteriori informazioni, vedere SSL e certificati 311.

Porte POP3/IMAP (alcune funzionalità richiedono MDaemon PRO)

Porta POP3 in entrata
MDaemon controlla questa porta per rilevare le connessioni in entrata da client POP remoti.

Porta POP3 in uscita
Questa porta viene utilizzata quando MDaemon ritira la posta da un server POP3.

Porta IMAP in entrata
MDaemon controlla questa porta per rilevare le richieste IMAP in entrata.

Porta SSL POP3
Si tratta della porta dedicata per i client di posta POP3 che utilizzano una connessione SSL (Secure Sockets Layer). Per ulteriori informazioni, vedere SSL e certificati 311.

Porta SSL IMAP
Si tratta della porta dedicata per i client di posta IMAP che utilizzano una connessione SSL (Secure Sockets Layer). Per ulteriori informazioni, vedere SSL e certificati 311.

Altre porte

Porta DNS in uscita
Specificare la porta che MDaemon deve utilizzare per l'invio e la ricezione di datagrammi da e verso il server DNS.

Porta LDAP
Questa porta viene utilizzata da MDaemon per trasmettere le informazioni relative ai database e alle rubriche destinate al server LDAP.

Vedere: Supporto delle rubriche LDAP 100

Porta WebAdmin
Indica la porta utilizzata da MDaemon per rilevare le connessioni WebAdmin 144.

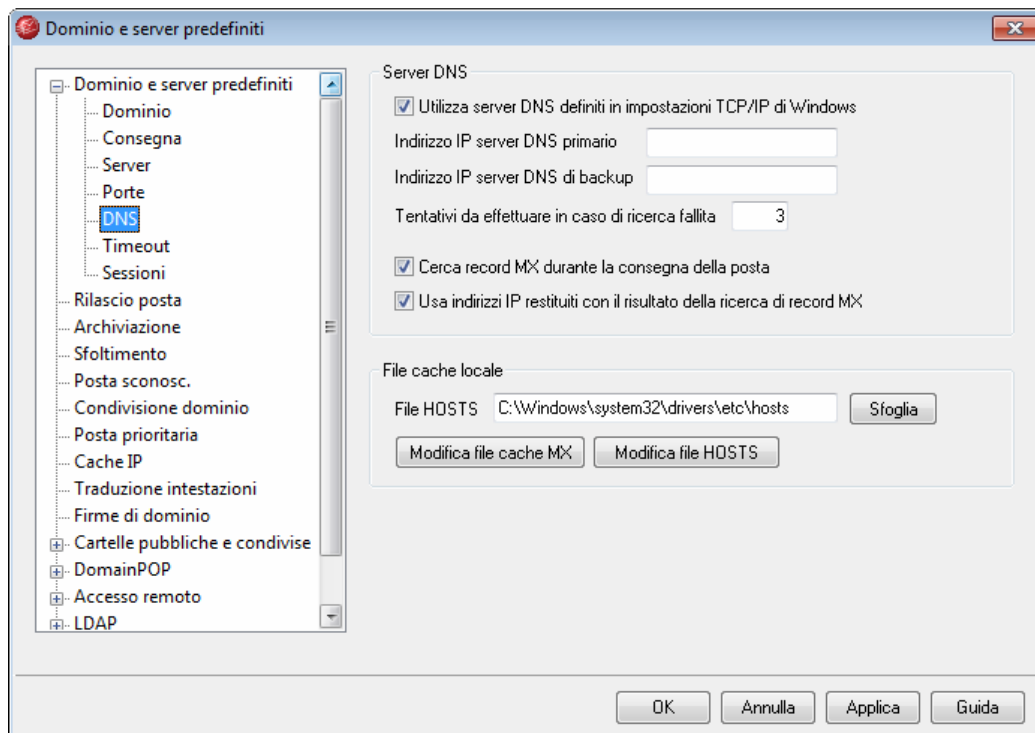
Porta Minger
Consente di specificare la porta monitorata dal server Minger 418 per le connessioni.

Ripristina impostazioni predefinite porte
Questo pulsante consente di ripristinare le impostazioni predefinite di tutte le porte.

Associa nuovi valori porta
Quando si modificano i valori di impostazione di una qualsiasi porta, è necessario premere questo pulsante per rendere immediatamente operative le modifiche apportate. In caso contrario, le modifiche non saranno operative se non dopo il riavvio del server.

Le impostazioni relative alle porte appena descritte rivestono un ruolo cruciale per il corretto funzionamento del server e non devono essere modificate, se non in caso di assoluta necessità. La conoscenza della configurazione delle porte usate da MDaemon è utile per collegare il server con sistemi proxy o altri software che richiedono la definizione di porte specifiche.

Ogni indirizzo IP, ossia ogni computer, dispone di diverse porte, ciascuna identificata univocamente. Se un programma tenta di accedere a una porta già utilizzata da un altro programma, un messaggio di errore informa l'utente che l'indirizzo richiesto (IP: PORTA) è già in uso.

4.1.1.5 DNS

Server DNS

Utilizza server DNS definiti in impostazioni TCP/IP di Windows
In alcuni casi Windows conserva un indirizzo IP del server DNS all'interno della configurazione TCP/IP locale. Se questo si verifica anche per il computer in uso, è possibile selezionare questa opzione. Se MDaemon non riesce a trovare un server DNS locale, continua la ricerca fino a utilizzare uno di quelli specificati in questa schermata.

Indirizzo IP server DNS primario
Questa casella consente di immettere l'indirizzo IP del server DNS in cui MDaemon deve ricercare eventuali record 'A' e 'MX'.

Indirizzo IP server DNS di backup
Questa casella consente di immettere l'indirizzo IP del server DNS secondario o di backup in cui MDaemon deve ricercare i record 'A' e 'MX'.

Tentativi da effettuare in caso di ricerca fallita
In questo campo viene indicato quante volte MDaemon deve ripetere il tentativo in caso di ricerca non riuscita. Se è stato definito un server DNS di backup, ciascun tentativo di ricerca viene effettuato su entrambi i server.

Cerca record MX durante la consegna della posta
Abilitare questa casella se si desidera che al momento di recapitare la posta MDaemon cerchi eventuali record 'MX' nei server DNS specificati.

Nelle opzioni di MDaemon in cui è consentito specificare un host a cui inoltrare, copiare o inviare posta è possibile utilizzare le convenzioni seguenti. Se l'host viene racchiuso tra parentesi (come in [esempio.com]), MDaemon ignorerà la ricerca di record MX al momento della consegna a tale host. Ad esempio, se l'opzione *Invia messaggio a questo host* della schermata Posta sconosciuta 65 contenesse "esempio.com", le ricerche MX verrebbero eseguite normalmente. Se, al contrario, tale opzione contenesse "[esempio.com]", verrebbe eseguita solo la ricerca di record A.

Usa indirizzi IP restituiti con il risultato della ricerca di record MX
Selezionare questa casella di controllo affinché MDaemon tenti di utilizzare gli indirizzi IP dei record 'A' rilevati durante le ricerche dei record 'MX'.

File cache locale

File HOSTS
Prima di interrogare i server DNS, MDaemon tenta di risolvere un indirizzo mediante il file HOSTS di Windows. Se nel file è presente l'indirizzo IP del dominio in questione, MDaemon non ricorre all'interrogazione del server DNS.

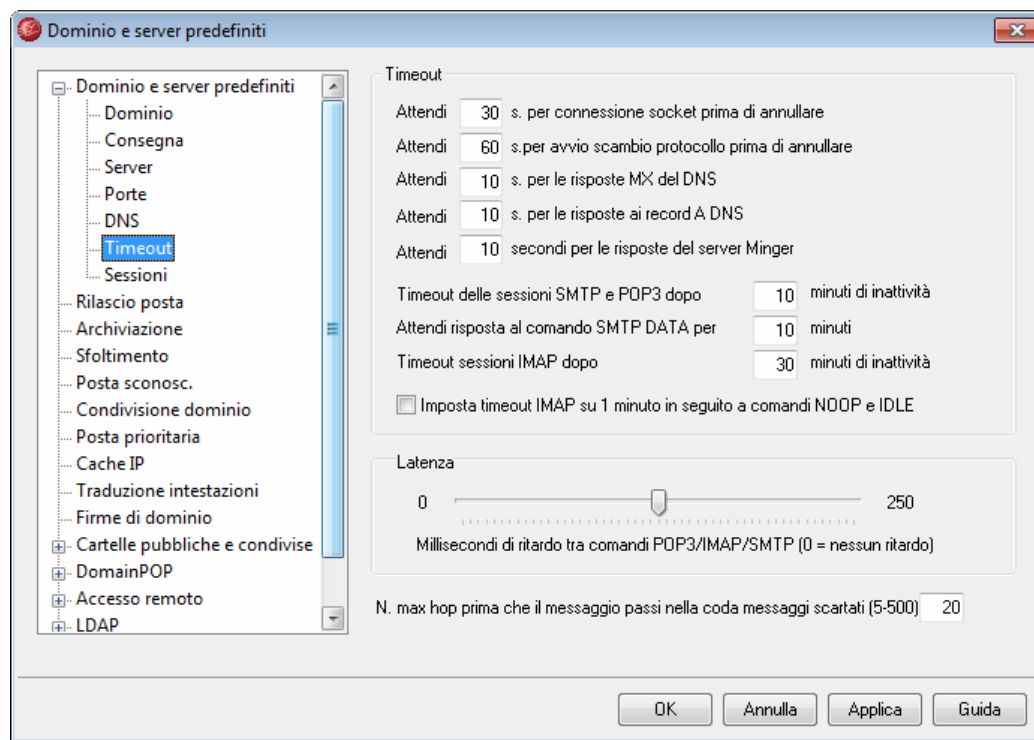
Oltre al nome, è necessario immettere anche il percorso completo del file. MDaemon tenta di utilizzare il valore riportato di seguito come posizione predefinita del file:

[unità]:\windows\system32\drivers\etc\hosts

Il file HOSTS è un file di Windows contenente il record A, ossia l'indirizzo IP principale relativo ai nomi di dominio. MDaemon consente inoltre di specificare gli indirizzi IP del record 'MX' all'interno del file MXCACHE.DAT presente nella sottodirectory MDaemon\APP\. Per ulteriori informazioni, aprire il file MXCACHE.DAT con un editor di testo e leggere i commenti presenti all'inizio del file.

Modifica file cache MX
Fare clic su questo pulsante per visualizzare o modificare il file MXCACHE.DAT utilizzando un editor di testo.

Modifica HOSTS
Fare clic su questo pulsante per visualizzare o modificare il file HOSTS utilizzando un editor di testo.

4.1.1.6 Timeout

Timeout

Attendi XX secondi per connessione socket prima di annullare
Una volta inoltrata una richiesta di connessione, MDaemon attende per un numero di secondi pari al valore specificato in questo campo che la connessione venga accettata dal sistema remoto. Se il sistema remoto non risponde entro questo intervallo di tempo, MDaemon invia il messaggio a un *server* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Dominio 41 dell'editor del dominio predefinito.

Attendi XX secondi per avvio scambio protocollo prima di annullare
Una volta stabilita la connessione a un host remoto, questo valore indica per quanti secondi MDaemon attende che l'host avvii lo scambio del protocollo SMTP o POP3. Se l'host remoto non avvia la sessione di protocollo entro questo intervallo di tempo, MDaemon invia il messaggio a un *server* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Dominio 41 dell'editor del dominio predefinito.

Attendi XX secondi per le risposte MX del DNS
Intervallo, espresso in secondi, in cui MDaemon attende la risposta relativa alla risoluzione degli host 'MX' per i domini remoti presso i servizi DNS interrogati. Se il server DNS non risponde entro questo intervallo di tempo, MDaemon tenta di consegnare il messaggio all'indirizzo IP specificato nel record DNS 'A' dell'host remoto. Se il tentativo non riesce, MDaemon invia il messaggio a un *server* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Dominio 41 dell'editor del dominio predefinito.

Attendi XX secondi per le risposte ai record A DNS
Questo timer determina il tempo di attesa di MDaemon perché venga restituito l'indirizzo IP di un host remoto. Se il tentativo non riesce, MDaemon invia il messaggio a un *server* specificato o lo colloca nella coda tentativi, a seconda dell'opzione scelta nella schermata Dominio 41 dell'editor del dominio predefinito.

Attendi XX secondi per le risposte del server Minger
Numero di secondi di attesa per la risposta del server Minger 418.

Timeout delle sessioni SMTP e POP3 dopo XX minuti di inattività
Se una connessione valida e operativa rimane inattiva (nessuno scambio) per questo intervallo di tempo, MDaemon chiude la transazione. MDaemon eseguirà un nuovo tentativo al successivo intervallo di elaborazione programmato.

Attendi risposta al comando SMTP DATA per XX minuti
Questa opzione gestisce il tempo per cui MDaemon resta in attesa della risposta "`250 Ok`" dopo l'invio del comando `DATA` durante l'elaborazione SMTP. Poiché alcuni server di ricezione eseguono in questa fase operazioni antispam, antivirus e altre operazioni necessarie che possono richiedere molto tempo, questa opzione può essere utilizzata per completare tali attività. Il valore predefinito è di 10 minuti.

Timeout sessioni IMAP dopo XX minuti di inattività
Trascorso questo intervallo di inattività, espresso in minuti, MDaemon chiude la sessione IMAP.

Imposta timeout IMAP su 1 minuto in seguito a comandi NOOP e IDLE

Se questa opzione è selezionata, il timer di inattività IMAP verrà impostato su un minuto ogni volta che viene trasmesso un comando NOOP o IDLE. Alcuni client IMAP trasmettono comandi NOOP solo per mantenere aperta una sessione, anche se non è in corso alcuna attività di trasmissione della posta. Questa funzione impedisce che tali sessioni rimangano attive impegnando le risorse necessarie ai siti di posta IMAP più voluminosi.

Latenza

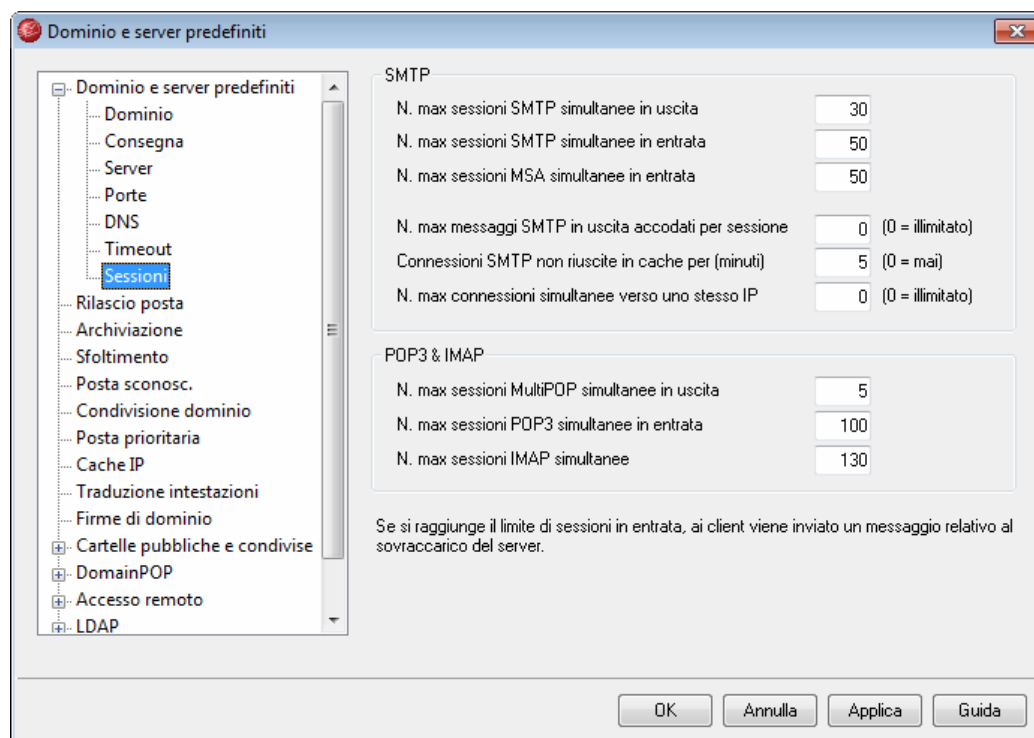
Latenza - XX millisecondi

Si tratta dell'intervallo di tempo che intercorre tra i comandi di protocollo POP/SMTP/IMAP. Questa funzione è utile per impedire che connessioni ad alta velocità elaborino i dati con una velocità superiore a quella con cui il destinatario è in grado di riceverli. Questo ritardo viene applicato solo alla sequenza dei comandi di protocollo POP/SMTP/IMAP: il trasferimento vero e proprio di un messaggio di posta è già completamente nei buffer.

Rilevamento e controllo loop

N. max hop prima che il messaggio passi nella coda messaggi scartati (5-500)

In base agli standard RFC, un server di posta è tenuto a contrassegnare ciascun messaggio ogni volta che questo viene elaborato. Questi contrassegni possono essere contati e utilizzati come misura provvisoria per evitare i loop di posta, che in alcuni casi sono causati da configurazioni errate. Se non vengono rilevati, questi loop di consegna dei messaggi esauriranno le risorse del sistema. Calcolando il numero di volte per cui un messaggio viene elaborato, è possibile rilevare tali messaggi e collocarli nella directory dei messaggi scartati. Si presuppone che sia in corso un loop di posta se un messaggio non ha raggiunto il destinatario dopo un certo numero di elaborazioni da parte dei server. L'impostazione predefinita di questo comando dovrebbe essere sufficiente a impedire il verificarsi di loop di posta.

4.1.1.7 Sessioni

SMTP

N. max sessioni SMTP simultanee in uscita
Il valore inserito in questo campo indica il numero massimo di sessioni SMTP in uscita che possono essere create al momento di inviare la posta. Ogni sessione trasmette i messaggi in uscita finché la coda non è vuota o non è stato raggiunto il valore indicato nel campo *N. max messaggi SMTP in uscita accodati per sessione*. Ad esempio, se è stato specificato il valore 5 e la coda della posta in uscita contiene 20 messaggi, al momento di inviare la posta vengono generate 5 sessioni simultanee, ciascuna delle quali trasmette consecutivamente 4 messaggi.

L'impostazione predefinita di questa opzione è 30, ma è possibile modificarlo per individuare l'impostazione più appropriata ai fini delle prestazioni in base alla larghezza di banda disponibile, evitando tuttavia di specificare un numero troppo alto che possa sovraccaricare la larghezza di banda e le risorse di Windows a scapito dell'efficienza di consegna. Tenere presente che in ciascuna sessione SMTP creata da MDaemon i messaggi vengono consegnati consecutivamente: per tale motivo, 4 sessioni che recapitano 2 messaggi ognuna offrono prestazioni migliori e più veloci di 8 sessioni che recapitano 1 messaggio ognuna. Un valido parametro di partenza potrebbe essere un valore compreso tra 5 e 10 sessioni per i modem a 56K e tra 10 e 20 per i modem a banda larga.

N. max sessioni SMTP simultanee in entrata
Questo valore controlla il numero di sessioni SMTP simultanee in entrata che il server accetta prima che ne venga segnalato il sovraccarico. Il valore predefinito è 50.

N. max sessioni MSA simultanee in entrata
Questa opzione consente di indicare il numero massimo consentito di sessioni simultanee MSA (Mail Submission Agent) in entrata.

N. max messaggi SMTP in uscita accodati per sessione
Questo parametro stabilisce un limite sul numero di singoli messaggi che verranno inviati in ciascuna sessione prima che si interrompa la consegna della posta e venga liberata la memoria. Di norma, questo valore deve essere impostato su zero, in modo che ciascuna sessione continui a consegnare i messaggi di posta fino a svuotare la coda.

Connessioni SMTP non riuscite in cache per (minuti)
Quando una connessione SMTP verso uno specifico host non riesce, MDaemon non esegue ulteriori tentativi di connessione all'host per il numero di minuti indicato nell'opzione. In tal modo è possibile evitare di tentare nuove connessioni verso un host non funzionante quando, ad esempio, sono presenti in coda numerosi messaggi indirizzati all'host e al primo tentativo di consegna si riscontra che l'host non è connesso. Il valore predefinito è di 5 minuti. Specificare "0" se non si desidera inserire nella cache gli errori SMTP.

N. max connessioni simultanee verso uno stesso IP (0 = illimitate)
Questa opzione consente di limitare il numero di connessioni simultanee verso uno stesso indirizzo IP durante la consegna della posta. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

Questa opzione si rivela utile per impedire l'esecuzione di un numero eccessivo di connessioni simultanee verso più indirizzi IP. In fase di consegna, se per un messaggio è necessaria una connessione a un indirizzo IP che determinerebbe il superamento del limite impostato, la connessione non viene eseguita e viene utilizzato il successivo host MX o il successivo host intelligente. Se mon sono disponibili ulteriori host, il messaggio viene accodato per il successivo ciclo di consegna. Per impostazione predefinita l'opzione è disattivata, in modo da mantenere il comportamento precedente del sistema. Sempre per impostazione predefinita, anche le connessioni verso gli indirizzi IP accreditati vengono escluse da questa funzionalità. Tuttavia, se si desidera applicarla anche agli IP accreditati, è possibile impostare la seguente opzione del file `MDaemon.ini`:

```
[Sessions]
TrustedIPsUseConnectionLimit=Yes (il valore predefinito è No)
```

Per impostazione predefinita, anche le connessioni verso indirizzi IP riservati per l'uso intranet vengono escluse da questa funzionalità. Si tratta degli indirizzi IP `127.0.0.*`, `192.168.*.*`, `10.*.*.*` e `172.16.0.0/12`. Tuttavia, se si desidera applicarla anche agli IP accreditati, è possibile impostare la seguente opzione del file `MDaemon.ini`:

```
[Sessions]
ReservedIPsUseConnectionLimit=Yes (il valore predefinito è No)
```

POP3 & IMAP

N. max sessioni MultiPOP simultanee in uscita

Si tratta del numero massimo di sessioni POP in uscita che possono essere generate al momento di raccogliere la posta MultiPOP. Ogni sessione raccoglie questo tipo di posta finché non sono stati controllati tutti i server MultiPOP e non è stata raccolta tutta la posta. Se ad esempio il valore specificato è 3 e le sessioni MultiPOP per tutti gli utenti sono 15, ciascuna sessione raccoglie la posta da 5 origini MultiPOP.

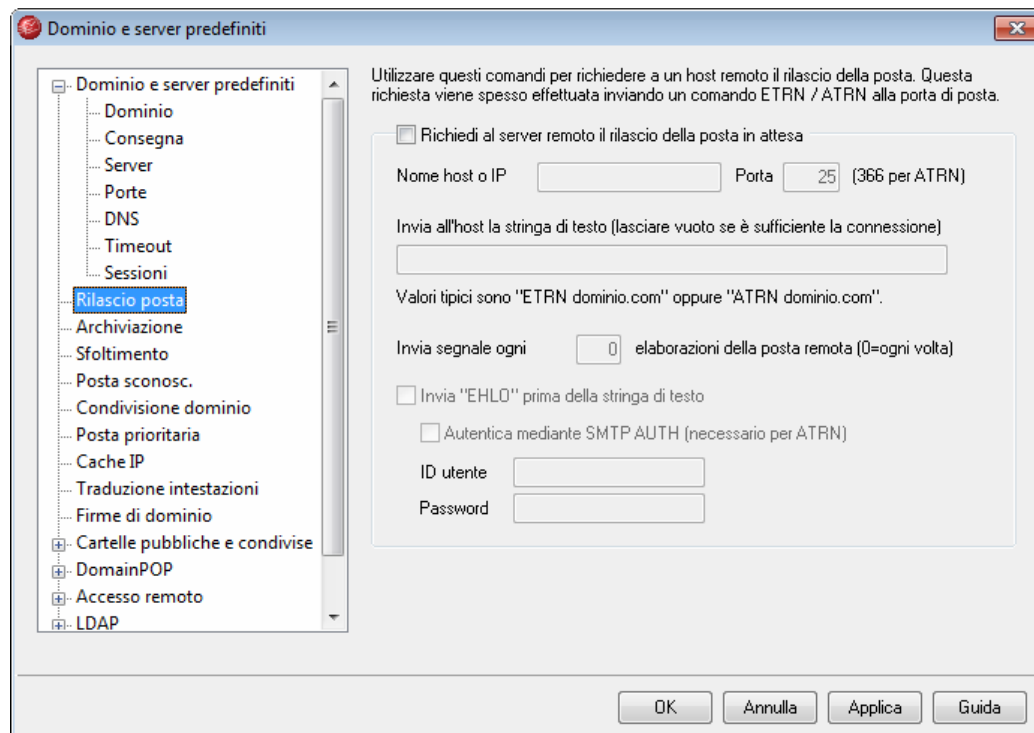
Si consiglia di eseguire più tentativi per rilevare quale numero di sessioni consenta di ottimizzare le prestazioni della larghezza di banda della rete, in modo da non specificare un numero troppo alto ed evitare di sovraccaricare la larghezza di banda o le risorse di Windows a scapito dell'efficienza di elaborazione. Tenere presente che ciascuna sessione POP generata da MDaemon procede alla raccolta della posta fino a svuotare tutte le origini. Pertanto, 4 sessioni che raccolgono la posta da 20 origini garantiscono prestazioni migliori e più veloci di 20 sessioni che raccolgono la posta da un'unica origine.

N. max sessioni POP3 simultanee in entrata

Questo valore controlla il numero massimo di sessioni POP simultanee in entrata consentite prima che il server segnali un sovraccarico.

N. max sessioni IMAP simultanee

Questo valore controlla il numero massimo di sessioni IMAP simultanee consentite prima che il server segnali un sovraccarico.

4.1.2 Rilascio posta

Richiedi al server remoto il rilascio della posta in attesa
Durante l'elaborazione della posta remota, MDaemon è in grado di connettersi a qualsiasi server o porta e inviare una stringa. Questa funzionalità si rivela particolarmente quando è necessario segnalare a un server remoto il rilascio della posta mediante una determinata stringa, ad esempio `ATRN`, `ETRN` o `QSND`. Questa funzione è efficace anche qualora l'ISP o l'host remoto richiedano una breve sessione `FINGER` o `TELNET` per verificare lo stato online del server in uso.

Nome host o IP
È l'host a cui è necessario inviare il segnale di rilascio della posta.

Porta
Specificare la porta da utilizzare per la connessione. Il valore predefinito 25 (porta SMTP) è adatto al metodo di segnalazione `ETRN` o `QSND`; la porta 366 viene di norma usata per la trasmissione di segnali `ATRN`, mentre la porta 79 per i segnali `FINGER`.

Invia all'host la stringa di testo (lasciare vuoto se è sufficiente la connessione)
In questo campo è possibile specificare la stringa di testo che deve essere trasmessa per il rilascio della posta. Ad esempio, il metodo `ETRN` richiede l'inserimento del testo "`ETRN`" seguito dal nome del dominio del sito in coda; altri metodi, invece, richiedono l'invio di stringhe diverse. Per ulteriori informazioni sulle stringhe da inviare per sbloccare la coda di posta, consultare l'ISP. Quando si utilizza un metodo di annullamento dell'accodamento basato su un host di posta, è consigliabile utilizzare il metodo ODMR (On-Domain Mail Relay) 60, se possibile. Per il metodo ODMR, utilizzare in questo campo il comando ATRN.

Invia segnale ogni [xx] elaborazioni della posta remota (0=ogni volta)
Per impostazione predefinita, il segnale di annullamento dell'accodamento viene trasmesso a ogni elaborazione della posta remota. Il valore immesso in questo campo consente di regolare la frequenza di invio del segnale, che avverrà per un numero di volte pari al valore impostato. Ad esempio, se il valore è "3", il segnale viene trasmesso ogni tre elaborazioni della posta remota.

Invia "EHLO" prima della stringa di testo
Se questa casella di controllo è selezionata, per richiedere il rilascio della posta è necessario connettersi a un server SMTP. Questa opzione fa in modo che, avviata una sessione SMTP con l'host specificato, la trasmissione della stringa di sblocco avvenga dopo l'invio dell'istruzione SMTP "EHLO".

Autenticazione prima di invio stringa di testo (richiesto per ATRN)
Come misura di sicurezza, per rilasciare i messaggi in attesa alcuni host o server richiedono l'autenticazione dei client mediante ESMTP AUTH. Se questo è il caso dell'host di posta, selezionare la casella di controllo e immettere le credenziali di autenticazione necessarie.

L'autenticazione viene richiesta quando si utilizza il comando ATRN per annullare l'accodamento della posta.

ID utente
Inserire il parametro ID utente AUTH richiesto dall'host.

Password
Inserire la password AUTH.

4.1.2.1 ODMR (On-Demand Mail Relay)

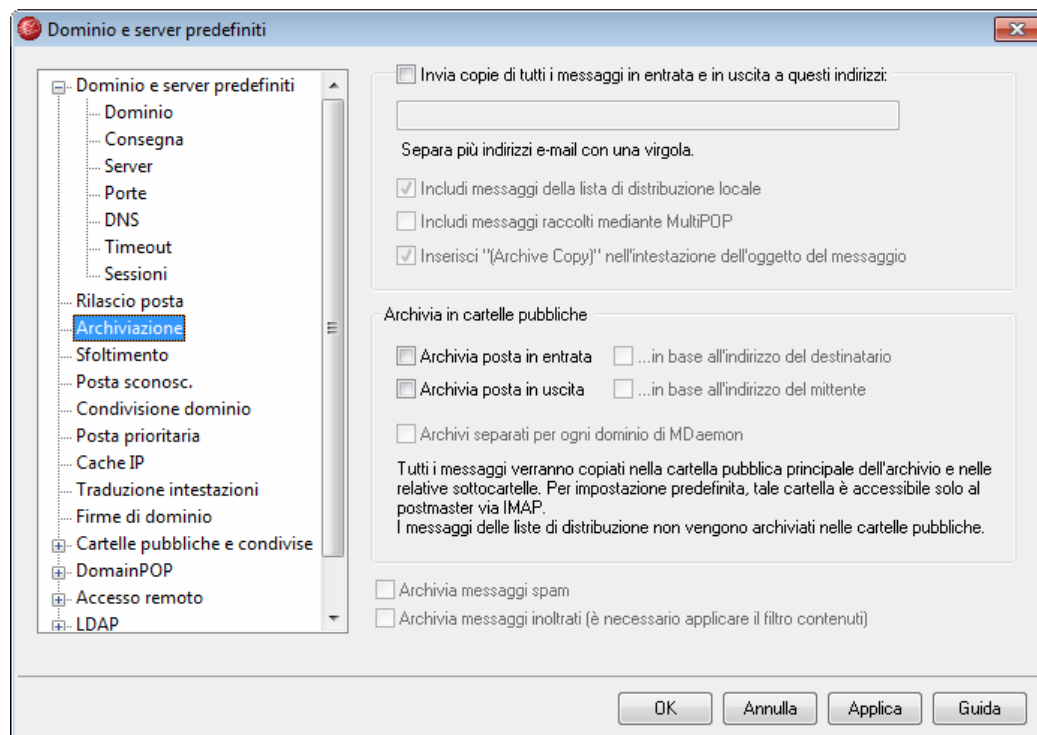
Se è necessario utilizzare un metodo di accodamento o annullamento dell'accodamento per l'hosting e il rilascio della posta, è consigliabile utilizzare il metodo ODMR (On-Domain Mail Relay), se possibile. Il metodo ODMR risulta superiore a ETRN e ad altri sistemi perché richiede un processo di autenticazione prima che venga eseguito il rilascio della posta. Inoltre, utilizza un comando ESMTP chiamato ATRN, in base al quale non è necessario che il client possegga un indirizzo IP statico, in quanto inverte il flusso di dati tra il client e il server e rilascia i messaggi senza dover effettuare una nuova connessione (a differenza di ETRN).

Dal lato client, MDaemon offre un supporto completo per ODMR mediante il comando ATRN e i comandi di autenticazione presenti nella scheda Rilascio posta 59. Per quanto riguarda il lato server, il supporto consiste in funzioni di gateway di dominio presenti nella schermata Annullamento dell'accodamento 467 di Gateway Editor.

Poiché alcuni server di posta non supportano ancora il metodo ODMR, è necessario verificarne la disponibilità presso il proprio provider prima di utilizzarlo.

Per ulteriori informazioni, vedere:

Gateway Editor » Annullamento dell'accodamento 467

4.1.3 Archiviazione

Invia copie di tutti i messaggi in entrata e in uscita a questi indirizzi
Inserire gli indirizzi ai quali inviare i messaggi da archiviare separandoli con una virgola. È possibile specificare indirizzi locali e remoti, nonché alias.

Includi messaggi della lista di distribuzione locale
Selezionare questa opzione per archiviare anche i messaggi delle liste di distribuzione.

Includi messaggi raccolti mediante MultiPOP
Questa opzione consente di archiviare i messaggi raccolti mediante la funzione MultiPOP 367 di MDaemon.

Inserisci "(Archive Copy)" nell'intestazione dell'oggetto del messaggio
Se si abilita questa opzione, nell'intestazione `Subject:` della posta archiviata viene inserita la dicitura "(Archive Copy)".

Archivia in cartelle pubbliche

Archivia posta in entrata
Selezionare questa casella di controllo per salvare una copia di tutti i messaggi in entrata nella cartella pubblica principale dell'archivio di posta e nelle relative sottocartelle. Per impostazione predefinita, tale cartella è accessibile solo dal postmaster via IMAP. Se si desidera modificare le autorizzazioni o accordare l'accesso a più utenti, utilizzare Elenco controllo accessi80 della schermata Elenco cartelle78 di Cartelle pubbliche e condivise.

...in base all'indirizzo del destinatario
Selezionare questa opzione per organizzare l'archivio della posta in entrata in base all'indirizzo e-mail del destinatario.

Archivia posta in uscita
Selezionare questa casella di controllo per salvare una copia di tutti i messaggi in uscita all'interno della cartella pubblica dell'archivio di posta. Per impostazione predefinita, tale cartella è accessibile solo dal postmaster via IMAP. Se si desidera modificare le autorizzazioni o accordare l'accesso a più utenti, utilizzare Elenco controllo accessi80 della schermata Elenco cartelle78 di Cartelle pubbliche e condivise.

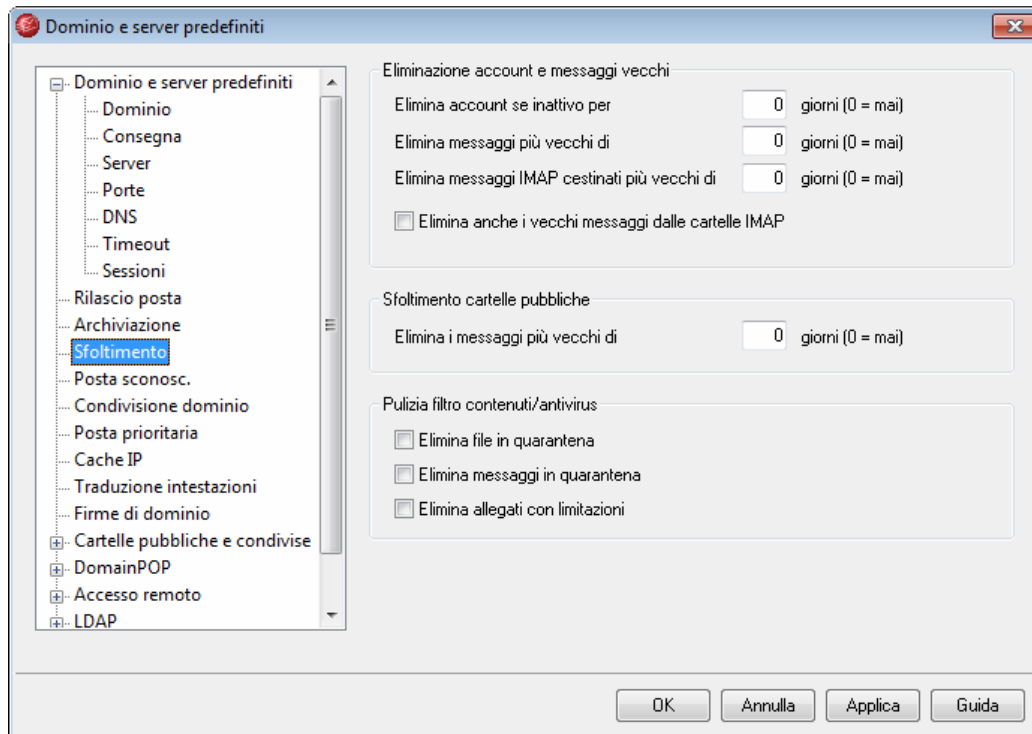
...in base all'indirizzo del mittente
Selezionare questa opzione per organizzare l'archivio della posta in uscita in base all'indirizzo e-mail del mittente.

Archivi separati per ogni dominio di MDaemon
Selezionare questa casella di controllo per disporre di un archivio separato per ogni dominio.

Impostazioni archivio

Archivia messaggi spam
Questa opzione consente di includere nell'archivio i messaggi contrassegnati come spam.

Archivia messaggi inoltrati (è necessario applicare il filtro contenuti)
Questa opzione consente di memorizzare i messaggi inoltrati che, per impostazione predefinita, non vengono archiviati.

4.1.4 Sfoltimento

I comandi presenti nella prima sezione di questa finestra di dialogo consentono di specificare se e quando MDaemon deve eliminare gli account inattivi o i vecchi messaggi appartenenti al dominio. Ogni giorno a mezzanotte MDaemon elimina tutti i messaggi e gli account che hanno superato i limiti di tempo impostati. Nella finestra di dialogo Domini aggiuntivi 114 sono presenti comandi analoghi che consentono di impostare questi limiti anche per altri domini. In Account Editor, inoltre, sono disponibili comandi per modificare queste impostazioni per i singoli account. Le opzioni rimanenti sono di tipo globale, valide per tutti i domini.

Quando i messaggi vecchi vengono sfoltiti anziché eliminati, MDaemon li sposta nella cartella "...\BADMSGS\[Casella]\", in cui possono essere eliminati manualmente in un secondo momento dall'amministratore o da un processo eseguito durante la notte. **Nota:** questa funzione è valida solo per i vecchi messaggi. Quando viene rimosso un account, questo non viene spostato, bensì eliminato insieme ai relativi messaggi. Per ulteriori informazioni e per le opzioni della riga di comando, vedere `AccountPrune.txt` nella cartella "...`MDaemon\App\`".

Eliminazione account e messaggi vecchi

Elimina account se inattivo per XX giorni (0 = mai)
Consente di specificare per quanti giorni un account del dominio può rimanere inattivo prima di essere eliminato. Specificando il valore "0", gli account non vengono

mai eliminati per inattività.

Elimina messaggi più vecchi di XX giorni (0 = mai)
Il valore di questo comando indica per quanti giorni un messaggio può rimanere nella casella postale di un utente prima di essere eliminato automaticamente. Se si immette il valore "0", i messaggi vecchi non vengono mai eliminati.

Elimina messaggi IMAP cestinati più vecchi di XX giorni (0 = mai)
Utilizzare questo comando per specificare per quanti giorni i messaggi IMAP contrassegnati per l'eliminazione devono rimanere nelle cartelle dell'utente. I messaggi contrassegnati per l'eliminazione che esistono da più di XX giorni vengono eliminati dalle rispettive caselle postali. Se si immette il valore "0", un messaggio vecchio contrassegnato per l'eliminazione non viene mai eliminato.

Elimina anche i vecchi messaggi dalle cartelle IMAP
Selezionare questa casella di controllo se si desidera applicare il comando "*Elimina i messaggi più vecchi di*" anche ai messaggi presenti nelle cartelle IMAP. Se questa opzione è disabilitata, i messaggi contenuti nelle cartelle IMAP non vengono eliminati, a prescindere dal periodo di permanenza nelle cartelle in questione.

Sfoltimento cartelle pubbliche

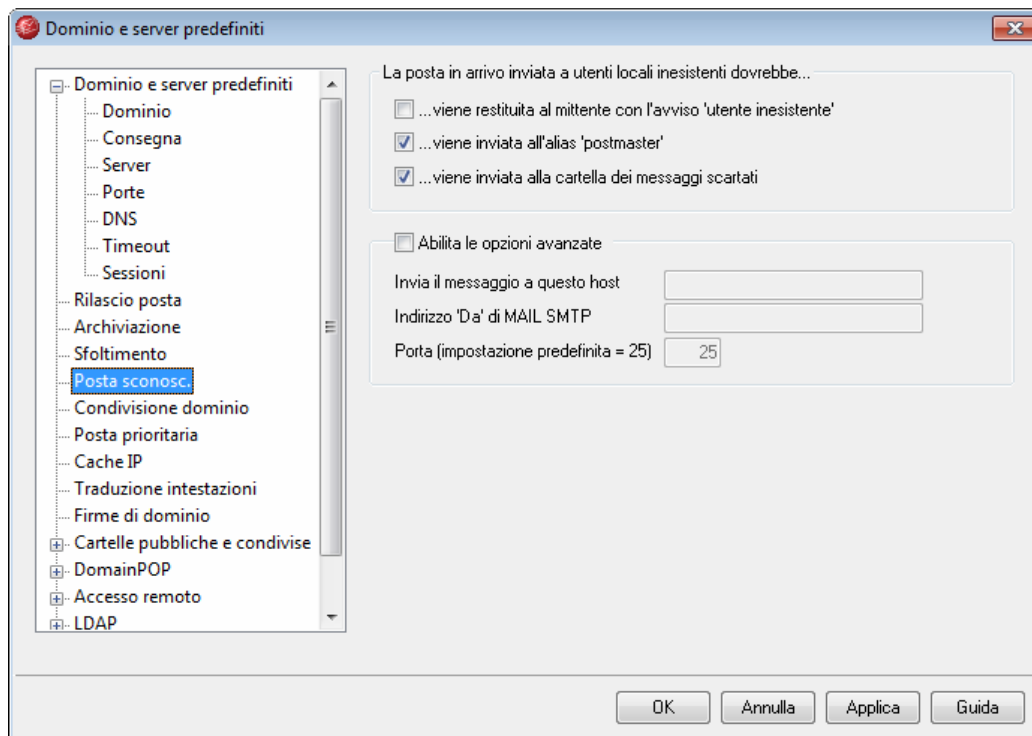
Elimina i messaggi più vecchi di XX giorni (0 = mai)
Per eliminare i messaggi vecchi dalle cartelle pubbliche, specificare il numero massimo di giorni di permanenza in questo campo.

Pulizia filtro contenuti/antivirus

Elimina file in quarantena
Selezionare questa opzione se si desidera che ogni notte vengano eliminati gli allegati in quarantena.

Elimina messaggi in quarantena
Selezionare questa opzione se si desidera che ogni notte vengano eliminati i messaggi in quarantena.

Elimina allegati con limitazioni
Selezionare questa opzione se si desidera che ogni notte vengano eliminati gli allegati con restrizioni.

4.1.5 Posta sconosciuta

La posta in arrivo inviata a utenti locali inesistenti...

...viene restituita al mittente con l'avviso 'utente inesistente'
Se questa opzione è abilitata, i messaggi recapitati al server e destinati a utenti presumibilmente locali ma sconosciuti vengono restituiti al mittente.

...viene inviata all'alias 'postmaster'
Abilitando questa opzione, selezionata per impostazione predefinita, i messaggi recapitati al server e destinati a utenti presumibilmente locali ma sconosciuti vengono inoltrati all'utente definito come postmaster. Se non si desidera inviare tali messaggi all'utente Postmaster, disabilitare questa opzione.

...viene inviata alla cartella dei messaggi scartati
Abiltando questa casella, selezionata per impostazione predefinita, i messaggi recapitati al server e destinati a utenti presumibilmente locali ma sconosciuti vengono collocati nella coda dei messaggi scartati. Se non si desidera inviare tali messaggi alla coda dei messaggi scartati, disabilitare questa opzione.

Opzioni avanzate

Abilita le opzioni avanzate
Selezionare questa casella di controllo per abilitare le proprietà avanzate di instradamento della posta.

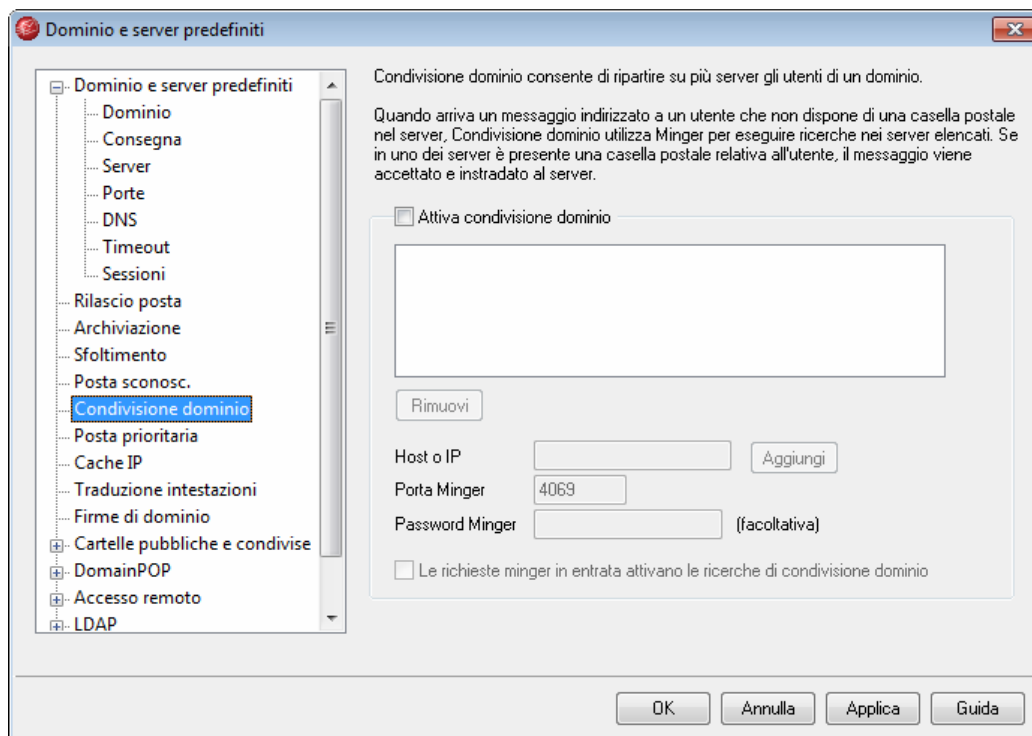
Invia il messaggio a questo host
I messaggi indirizzati a utenti locali sconosciuti vengono inviati all'host di posta il cui

nome è specificato in questo campo.

Nelle opzioni di MDaemon in cui è consentito specificare un host a cui inoltrare, copiare o inviare posta è possibile utilizzare le convenzioni seguenti. Se l'host viene racchiuso tra parentesi quadre (ad esempio, `[esempio.com]`) MDaemon ignorerà la ricerca di record MX al momento della consegna a tale host. Ad esempio, se tale opzione contenesse "`esempio.com`", le ricerche MX verrebbero eseguite normalmente. Se, al contrario, tale opzione contenesse "`[esempio.com]`", verrebbe eseguita solo la ricerca di record A.

Indirizzo 'Da' di MAIL SMTP
Questo indirizzo viene utilizzato nell'istruzione SMTP "`Mail From:`" durante l'handshake della sessione con l'host di destinazione. Di norma, in questa sezione della busta SMTP viene indicato il mittente del messaggio. Se è necessario utilizzare un comando vuoto (`MAIL FROM <>`), inserire nel campo la stringa "`[trash]`".

Porta
Indicare la porta TCP da utilizzare per l'invio del messaggio in sostituzione della porta predefinita SMTP per la posta in uscita.

4.1.6 Condivisione dominio

La condivisione del dominio è una funzione che consente di ripartire tra più server gli utenti del dominio predefinito[41] e dei domini aggiuntivi[114]. In tal modo, i server MDaemon possono essere eseguiti in postazioni diverse, utilizzando tutti gli stessi nomi di dominio, ma con account utente diversi. Parte degli account utente del dominio si trova in un server, mentre un'altra in uno o più altri server. La finestra di dialogo Condivisione dominio consente di specificare la posizione di ciascuno degli altri server. Quando arriva un messaggio per un utente locale privo di casella postale locale, Condivisione dominio esegue una query negli altri server mediante Minger per stabilire se l'utente dispone di un account in uno di essi. Se l'indirizzo si dimostra valido, MDaemon accetta il messaggio e lo instrada al server nel quale si trova l'account.

Se, ad esempio, si sceglie di utilizzare Condivisione dominio per uffici distribuiti in varie città è possibile offrire a ogni dipendente un indirizzo e-mail che termina con "`@esempio.com`." Il server MDaemon di ciascun ufficio ospiterà solo una parte dei messaggi di e-mail di `esempio.com`, relativa agli account dei dipendenti locali che lavorano in quell'ufficio. Per ogni ufficio, quindi, viene configurato Condivisione dominio in modo che ogni messaggio venga instradato all'ufficio appropriato.

Poiché Condivisione dominio verifica gli indirizzi utilizzando il server Minger[418], per il funzionamento della query è necessario aver abilitato e configurato correttamente Minger in ciascun server. Se, tuttavia, si verifica un errore durante la query Minger, ad esempio nel caso uno dei server sia temporaneamente non disponibile, MDaemon risponde con il codice di errore temporaneo "451", in modo che il server mittente possa tentare di recapitare nuovamente il messaggio in seguito. Quando un indirizzo è stato verificato, inoltre, viene memorizzato nella cache per cinque giorni in modo che MDaemon possa accettare subito i messaggi successivi per quell'indirizzo e instradarli all'host appropriato.

Per evitare, infine, i potenziali problemi che potrebbero verificarsi qualora si crei lo stesso account in più server, prima della creazione di un nuovo account viene eseguita una query in tutti i server di Condivisione dominio.

Esiste un'opzione denominata "*Le ricerche di verifica Minger attivano anche le ricerche di condivisione dominio*," che si trova nella schermata Opzioni[472] di Gateway Editor. Questa opzione consente di far sì che MDaemon esegua una query anche negli host di Condivisione dominio ogniqualvolta un gateway utilizzi la verifica Minger[462].

Abilita Condivisione dominio
Per attivare Condivisione dominio, selezionare questa casella di controllo. Dopo aver abilitato Condivisione dominio e aver aggiunto all'elenco tutti gli host o gli indirizzi IP di Condivisione dominio, assicurarsi che anche Minger[418] sia stato abilitato e configurato in modo da poter rispondere alle query degli host che tentano di verificare gli indirizzi locali.

Rimuovi
Per eliminare una delle voci di Condivisione dominio, selezionarla nell'elenco e fare clic su questo pulsante.

Host o IP
In questa casella è possibile inserire l'host o l'indirizzo IP che condivide uno o più domini. Se per l'invio di messaggi SMTP all'host si desidera utilizzare una porta specifica che non sia quella predefinita, è possibile aggiungere il carattere due punti e il numero di una porta, ad esempio `posta.esempio.com:2525`. Questa porta differisce dalla porta Minger.

Porta Minger
Porta utilizzata da Minger per le query all'host. La porta predefinita è 4069.

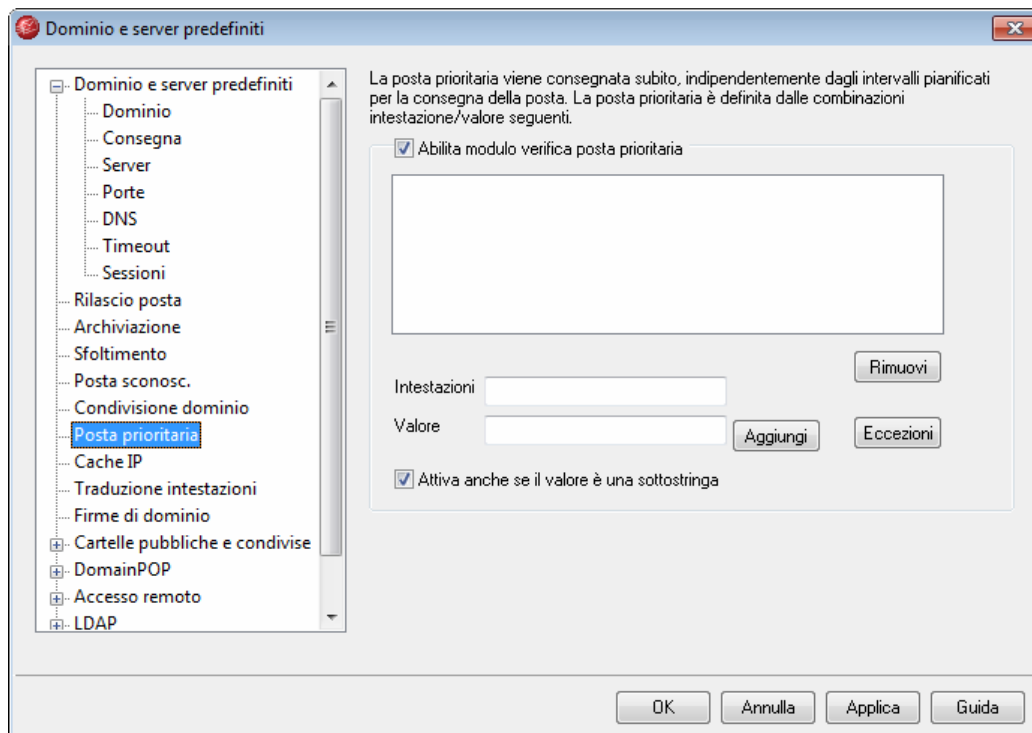
Password Minger (facoltativa)
È possibile inserire la password Minger eventualmente necessaria per l'host aggiunto. L'impostazione di Minger per la richiesta di una password è facoltativa, ma consigliata.

Aggiungi
Dopo aver inserito l'host o l'indirizzo IP, la porta e la password, fare clic su questo pulsante per aggiungere all'elenco la nuova voce di Condivisione dominio.

Le richieste minger in entrata attivano le ricerche di condivisione dominio
Se si abilita questa opzione, le richieste minger in entrata restituiscono TRUE quando un altro nodo di pari livello della rete di condivisione dominio stabilisce che accetterà il messaggio, anche se tale nodo non dispone effettivamente della casella postale locale. L'opzione è disabilitata per impostazione predefinita.

Vedere:

Minger 418
Dominio predefinito 41
Domini aggiuntivi 114

4.1.7 Posta prioritaria

Per accedere alla schermata Posta prioritaria, selezionare "Impostazioni » Dominio predefinito/server » Posta prioritaria". Questa schermata consente di definire le caratteristiche della posta prioritaria nel sistema. La posta prioritaria viene immediatamente consegnata da MDaemon, indipendentemente dagli intervalli pianificati per l'elaborazione della posta. All'arrivo di un nuovo messaggio, MDaemon lo analizza per confrontarne le intestazioni con le varie combinazioni intestazione/valore specificate in questa finestra di dialogo. Se riscontra una corrispondenza, MDaemon considera il messaggio come missiva di elevata priorità e tenta di consegnarlo immediatamente.

Posta prioritaria

Abilita modulo verifica posta prioritaria
Selezionare questa casella di controllo per abilitare la funzione Posta prioritaria. MDaemon verificherà lo stato di priorità dei messaggi in entrata.

Intestazione
Immettere in questo campo l'intestazione del messaggio. Non includere il carattere finale di due punti (:).

Valore
Immettere in questo campo il valore da ricercare nell'intestazione specificata che, se presente, attribuisce al messaggio una priorità elevata.

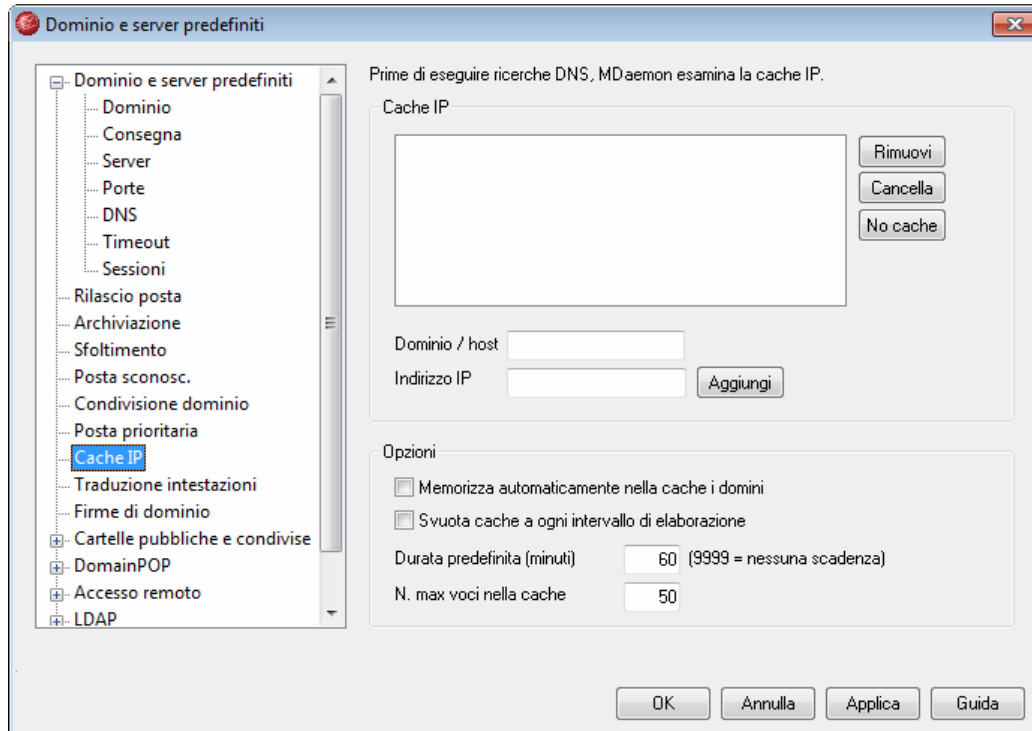
Attiva anche se il valore è una sottostringa
Quando si immette una nuova impostazione relativa al livello di priorità della posta, è possibile selezionare questa funzione per verificare anche una porzione (o

sottostringa) del valore di un'intestazione. Ad esempio, si supponga di avere creato un'impostazione di posta prioritaria in cui l'intestazione "`To`" è associata al valore "`Boss`". In questo modo, viene considerata posta prioritaria tutta la posta contenente "`Boss@qualunquedominio`" nell'intestazione. Se questa funzione non è abilitata, il valore dell'intestazione deve corrispondere esattamente al valore specificato nel campo: la corrispondenza di una porzione non è sufficiente.

Aggiungi
Una volta immesse le informazioni intestazione/valore nelle caselle di testo specificate e indicato se tali informazioni devono essere valide anche per le sottostringhe, fare clic su *Aggiungi* per creare la nuova voce di posta prioritaria.

Rimuovi
Fare clic su questo pulsante per rimuovere una voce selezionata dalla finestra *Intestazione/valore per posta prioritaria*.

Eccezioni
Questo pulsante consente di definire combinazioni intestazione/valore in base alle quali un messaggio verrà considerato come un'eccezione alle impostazioni di posta prioritaria. La funzione può quindi essere adattata alle più svariate situazioni.

4.1.8 Cache IP

Per velocizzare la consegna dei messaggi e ridurre i tempi di elaborazione della posta, MDaemon memorizza tutti gli indirizzi IP rilevati nella cache. La cache viene controllata

ogni volta che MDaemon richiede informazioni DNS per un nome dominio. Se il nome dominio in attesa di risoluzione si trova all'interno della cache degli indirizzi IP, la ricerca DNS viene annullata, in modo da ridurre i tempi di elaborazione. Le impostazioni di questa finestra consentono di controllare i parametri operativi della cache. Alcune operazioni, ad esempio l'aggiunta e la rimozione di voci, la definizione della dimensione massima della cache e la durata della permanenza nella cache possono essere eseguite manualmente. Per accedere alla cache degli indirizzi IP, selezionare "Impostazioni » Dominio predefinito/server » Cache IP".

Cache IP

Dominio / host
Immettere il nome dominio da aggiungere alla cache degli indirizzi IP.

IP
Immettere l'indirizzo IP da aggiungere alla cache.

Aggiungi
Dopo aver immesso il nome dominio o l'host e l'indirizzo IP, fare clic su questo pulsante per aggiungerli alla cache.

Rimuovi
Se si desidera rimuovere un indirizzo dalla cache IP, selezionarlo e fare clic su questo pulsante.

Cancella
Questo pulsante consente di eliminare tutte le voci inserite nella cache IP.

No cache
Fare clic su questo pulsante per visualizzare l'elenco di nomi domini e/o indirizzi IP da non memorizzare mai nella cache.

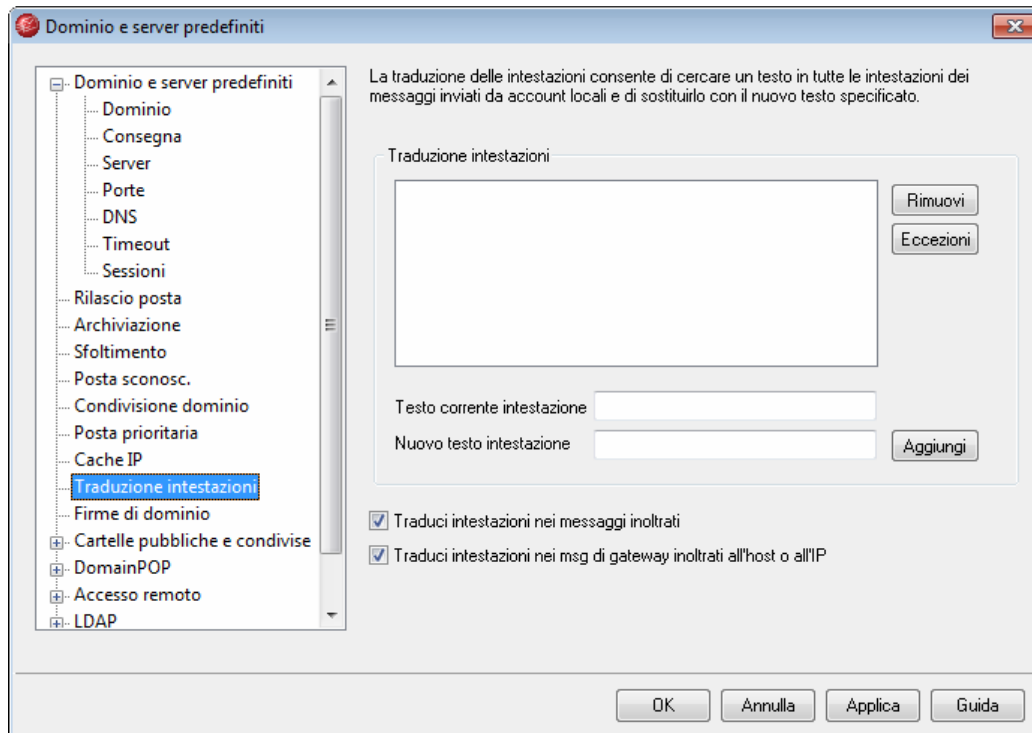
Opzioni

Memorizza automaticamente nella cache i domini
Questa opzione controlla il modulo interno di memorizzazione automatica nella cache di MDaemon: se si seleziona la casella di controllo, MDaemon memorizza automaticamente i domini nella cache. Per inserire manualmente le voci nella cache, deselezionare la casella.

Svuota cache a ogni intervallo di elaborazione
Se questa opzione è selezionata, l'intero contenuto della cache viene cancellato all'avvio di ogni sessione di posta. In questo modo, la cache viene aggiornata a ogni intervallo di elaborazione.

Durata predefinita (minuti)
Rappresenta il valore predefinito, in minuti, per la permanenza della voce nella cache degli indirizzi IP. Una volta trascorso questo intervallo, MDaemon rimuove la voce dalla cache. Per preservare la voce nella cache in modo permanente, immettere in questo campo il valore 9999.

N. max voci nella cache
Questo valore definisce la dimensione della cache. Una volta raggiunto il limite, se nella cache viene inserita una nuova voce, la prima (a livello cronologico) verrà rimossa.

4.1.9 Traduzione intestazioni

La funzione Traduzione intestazione consente di modificare qualsiasi porzione del testo dell'intestazione di un messaggio in uscita dal dominio verso un host remoto. È sufficiente specificare il testo da ricercare e il valore corrispondente con cui sostituirlo. MDaemon ricerca il testo in tutte le intestazioni dei messaggi e ne sostituisce ogni occorrenza con il valore specificato. È inoltre possibile specificare le intestazioni che **non** devono essere modificate (ad esempio, "Subject:" o "Received:"). A tale scopo, fare clic sul pulsante *Eccezioni* della finestra di dialogo.

Questa funzione è necessaria per alcune configurazioni di MDaemon in cui il nome dominio locale è fittizio o diverso da quello che deve figurare nella posta in uscita. In tali situazioni, la funzione Traduzione intestazione può essere efficacemente utilizzata per modificare ogni occorrenza di "`@dominiolocale.com`" in "`@dominioremoto.com`".

Traduzione intestazioni
In questo elenco sono contenute le porzioni di testo da ricercare nelle intestazioni dei messaggi in uscita, nonché il testo che sostituirà la porzione eventualmente rilevata.

Rimuovi
Selezionare una voce nell'elenco Traduzione intestazioni, quindi fare clic su questo pulsante per rimuoverla.

Eccezioni
Fare clic su questo pulsante per aprire la finestra di dialogo Eccezioni alla traduzione intestazioni 73 e specificare le intestazioni da escludere dal processo di traduzione.

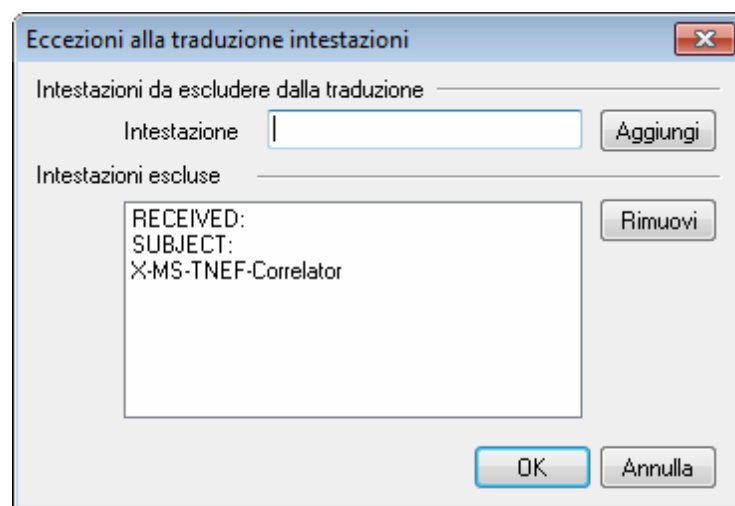
Testo corrente intestazione
Immettere il testo da sostituire nelle intestazioni dei messaggi in uscita.

Nuovo testo intestazione
Questo testo sostituisce quello specificato nel campo *Testo corrente intestazione*.

Aggiungi
Fare clic su questo pulsante per aggiungere i nuovi parametri all'elenco *Traduzione intestazioni*.

Traduci intestazioni nei messaggi inoltrati
Selezionare questa casella di controllo per eseguire le traduzioni delle intestazioni anche per i messaggi automaticamente inoltrati da un dominio locale a un dominio esterno.

Traduci intestazioni nei msg di gateway inoltrati all'host o all'IP
Selezionare questa casella di controllo se si desidera che le intestazioni vengano convertite nei messaggi inoltrati sul gateway di dominio. Per ulteriori informazioni, vedere la schermata Inoltro 466 di Gateway Editor.

4.1.9.1 Eccezioni alla traduzione intestazioni

Intestazioni da escludere dalla traduzione

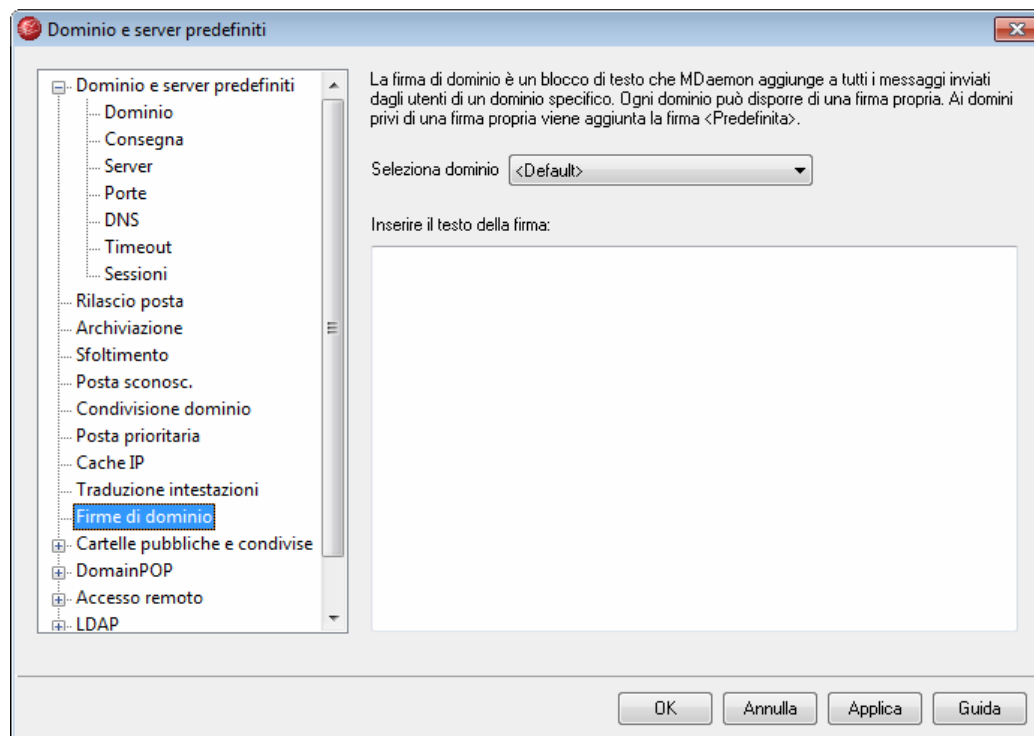
Intestazione
Immettere l'intestazione da escludere dal processo di traduzione delle intestazioni 72
.

Aggiungi
Fare clic su questo pulsante per aggiungere una nuova intestazione all'elenco.

Intestazioni escluse

Le intestazioni indicate verranno escluse dalla ricerca e dalla sostituzione del testo.

Rimuovi
Selezionare un'intestazione nell'elenco, quindi fare clic su questo pulsante per rimuoverla.

4.1.10 Firme di dominio

Questa finestra di dialogo consente di creare con estrema facilità un testo per la firma dei messaggi sia di tipo predefinito sia in base al dominio. Se esiste, il testo della firma predefinita viene allegato a tutti i messaggi inviati dagli utenti locali, a meno che per il dominio specifico dell'utente sia stato indicato un testo alternativo. Se disponibile, quest'ultimo avrà priorità sul testo predefinito. Le firme di dominio vengono aggiunte sempre in fondo ai messaggi. Tuttavia, nelle liste di distribuzione che utilizzano il pié di pagina, questo viene aggiunto al di sotto della firma di dominio.

Per aggiungere singole firme per ogni account è inoltre possibile utilizzare la funzione Firma 373 di Account Editor. Le firme dell'account vengono inserite prima di quelle del dominio.

4.1.11 Cartelle pubbliche e condivise

MDaemon supporta la condivisione delle cartelle IMAP sia pubbliche sia a livello di utente. Le cartelle pubbliche sono cartelle supplementari che non appartengono ad alcun account in particolare ma possono essere rese disponibili per più utenti IMAP. Le cartelle utente sono cartelle IMAP che appartengono a singoli account di MDaemon. A ciascuna cartella condivisa, pubblica o a livello di utente, deve essere associato un elenco di utenti di MDaemon e solo i membri di tale lista possono accedere a essa mediante WorldClient o un client e-mail IMAP.

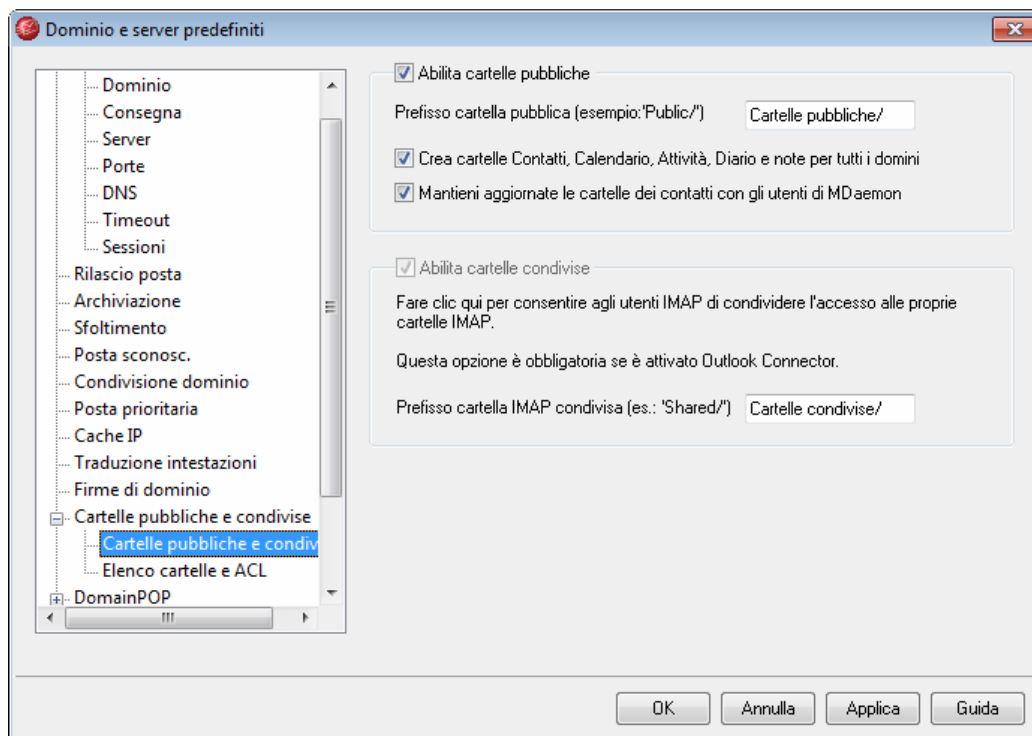
Quando gli utenti IMAP accedono all'elenco delle cartelle personali, visualizzano anche le cartelle pubbliche condivise e le cartelle utente condivise a cui possono accedere. In questo modo, è possibile che alcune cartelle di posta vengano condivise da più utenti e che vengano anche richieste le credenziali di connessione di ogni singolo utente. Inoltre, avere accesso a una cartella non significa necessariamente godere di un accesso completo di lettura/scrittura o amministrativo. I diritti di accesso specifici possono essere accordati ai singoli utenti, con possibilità di impostare per ciascuno di essi un livello di accesso diverso. Ad esempio, è possibile autorizzare solo alcuni utenti a eliminare i messaggi.

Dopo avere creato una cartella pubblica o utente, è possibile utilizzare la funzione Filtro contenuti per impostare i criteri secondo cui determinati messaggi vengono spostati in essa. Ad esempio, una regola utile potrebbe essere quella di spostare nella cartella pubblica `Assistenza` i messaggi contenenti `assistenza@dominio.com` nell'intestazione `TO:`. Le azioni di Filtro contenuti 214 "`Move Message to a Public Folder`" e "`Copy the Message to Folder`" lo consentono. Per le cartelle utente condivise, è possibile utilizzare i filtri IMAP personali 353 per instradare a esse messaggi specifici. Oltre a utilizzare Filtro contenuti e i filtri IMAP, è possibile associare un account specifico a una cartella condivisa in modo che i messaggi destinati a tale "indirizzo di invio" vengano instradati automaticamente alla cartella condivisa. Tuttavia, solo gli utenti a cui sia stata accordata l'autorizzazione a inviare nella cartella sono in grado di effettuare invii a tale indirizzo.

Per maggiore comodità, anche l'editor della lista di distribuzione contiene una schermata Cartelle pubbliche 445 che consente di associare una cartella pubblica a una lista specifica. Se questa funzione è abilitata, una copia di ciascun messaggio della lista viene collocata nella cartella pubblica specifica. Tutte le cartelle pubbliche vengono memorizzate nella directory `\Public Folders\` all'interno della gerarchia delle directory di MDaemon.

Per ulteriori informazioni, vedere:

[Cartelle pubbliche e condivise](76)
[Elenco cartelle](78)
[Elenco controllo accessi](80)
[Account Editor » Cartelle condivise](369)

4.1.11.1 Cartelle pubbliche e condivise

Per aprire la schermata Cartelle pubbliche e condivise, fare clic su "Impostazioni » Dominio predefinito/server » Cartelle pubbliche e condivise".

Cartelle pubbliche

Abilita cartelle pubbliche
Fare clic su questa casella di controllo per consentire agli utenti IMAP di accedere alle cartelle pubbliche. Gli utenti autorizzati ad accedere a tali cartelle e il livello di accesso accordato vengono specificati sotto ogni cartella nella schermata [Elenco cartelle](78). Deselezionare questa casella di controllo se si desidera nascondere le cartelle pubbliche a tutti gli utenti.

Prefisso cartella pubblica (esempio:'Public/')
Le cartelle pubbliche sono precedute da una sequenza composta da un massimo di 20 caratteri, ad esempio "#" o "Cartelle pubbliche/". In questo modo, gli utenti possono distinguere facilmente le cartelle pubbliche da quelle private del client e-

mail. Utilizzare questa casella di testo per specificare la serie di caratteri da usare per contrassegnare le cartelle pubbliche.

Crea cartelle Contatti, Calendario, Attività, Diario e note per tutti i domini
Fare clic su questa casella di controllo se si desidera garantire che le cartelle esistano per tutti i domini. Le cartelle vengono create ogni qualvolta si aggiunge a MDaemon un dominio aggiuntivo 115.

Mantieni cartelle di contatti aggiornate con gli utenti MDaemon
Se questa opzione è selezionata, MDaemon manterrà le cartelle dei contatti sincronizzate con l'elenco degli account.

Cartelle condivise

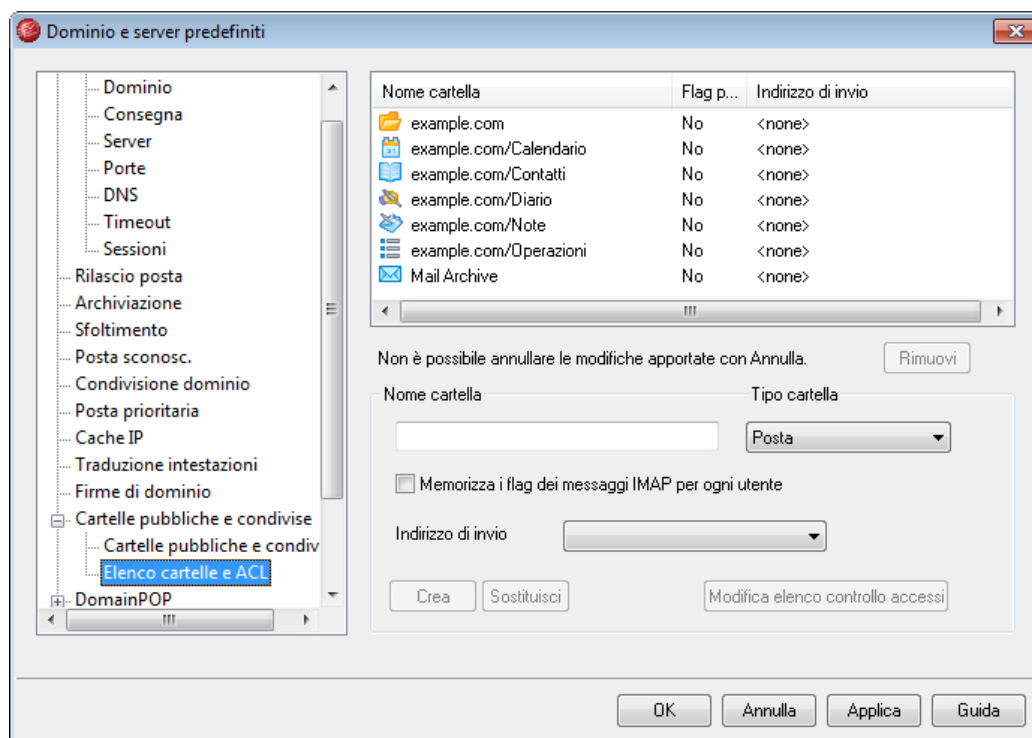
Abilita cartelle condivise
Fare clic su questa casella di controllo per consentire agli utenti IMAP di condividere l'accesso alle proprie cartelle IMAP. Gli utenti autorizzati ad accedervi e il livello di accesso accordato vengono specificati in base a ogni cartella nella schermata Cartelle condivise 369 di Account Editor, disponibile in Account » Account Manager » [Account utente] » Cartelle condivise. Deselezionare questa casella di controllo se si desidera impedire agli utenti la condivisione dell'accesso alle proprie cartelle e la visualizzazione della schermata Cartelle condivise in Account Editor.

Se si usa Outlook Connector per MDaemon, questa opzione non è disponibile. Non è possibile disattivarla poiché la condivisione delle cartelle utente è indispensabile per il corretto funzionamento di Outlook Connector.

Prefisso cartella IMAP condivisa (es.:'Condiv/')
Le cartelle pubbliche sono precedute da una sequenza composta da un massimo di 20 caratteri, ad esempio "`Cartelle pubbliche/`". In questo modo, gli utenti possono distinguere facilmente le cartelle condivise da quelle private del client e-mail. Utilizzare questa casella di testo per specificare la serie di caratteri da usare per contrassegnare le cartelle utente condivise.

Vedere:

Elenco cartelle 78
Elenco controllo accessi 80
Account Editor » Cartelle condivise 369

4.1.11.2 Elenco cartelle

Per aprire la schermata Elenco cartelle, fare clic su "Impostazioni » Dominio predefinito/server » Cartelle pubbliche e condivise » Elenco cartelle/ ACL".

Cartelle IMAP

In quest'area vengono visualizzate tutte le cartelle IMAP pubbliche create, l'impostazione dei *flag a livello di utente* e l'eventuale indirizzo di invio associato.

Rimuovi
Per rimuovere una cartella IMAP pubblica dall'elenco, selezionarla e fare clic sul pulsante Rimuovi.

Nuova cartella IMAP

Nome cartella
Per aggiungere una nuova cartella all'elenco, indicarne il nome nel campo, impostare le opzioni relative a *tipo di cartella*, flag a livello di utente e *indirizzo di invio*, quindi fare clic su *Crea*. Se si desidera che la nuova cartella sia una sottocartella di una di quelle in elenco, fare precedere al nome della nuova cartella il nome di quella principale e il carattere barra. Se, ad esempio, la cartella principale è denominata "`Cartella personale`" e la nuova cartella "`Nuova cartella personale`," il nome della nuova sottocartella sarà "`Cartella personale/Nuova cartella personale`". Se non si desidera che sia una sottocartella, assegnarle il nome "`Nuova cartella personale`" senza prefisso.

Tipo cartella
Utilizzando l'elenco a discesa, indicare il tipo di cartella: Posta, Contatti, Calendario e così via.

Memorizza i flag dei messaggi IMAP per ogni utente
Fare clic su questa casella di controllo se si desidera impostare i flag dei messaggi della cartella (letto, non letto, risposto a, inoltrato e così via) a livello di singolo utente anziché a livello globale. Ciascun utente visualizza lo stato dei messaggi nella cartella condivisa in base alla propria interazione personale. Un utente che non abbia letto un messaggio lo visualizzerà contrassegnato come 'non letto' mentre un utente che lo abbia letto lo visualizzerà come 'letto'. Se questo comando è disabilitato, tutti gli utenti visualizzano lo stesso stato. Pertanto, una volta che un utente ha letto un messaggio, anche tutti gli altri lo visualizzano come 'letto'.

Indirizzo di invio
Utilizzare questo elenco a discesa per associare un account specifico a una cartella condivisa in modo che i messaggi destinati a tale "indirizzo di invio" vengano instradati automaticamente alla cartella condivisa. Tuttavia, solo gli utenti a cui sia stata accordata l'autorizzazione a inviare nella cartella sono in grado di effettuare invii a tale indirizzo.

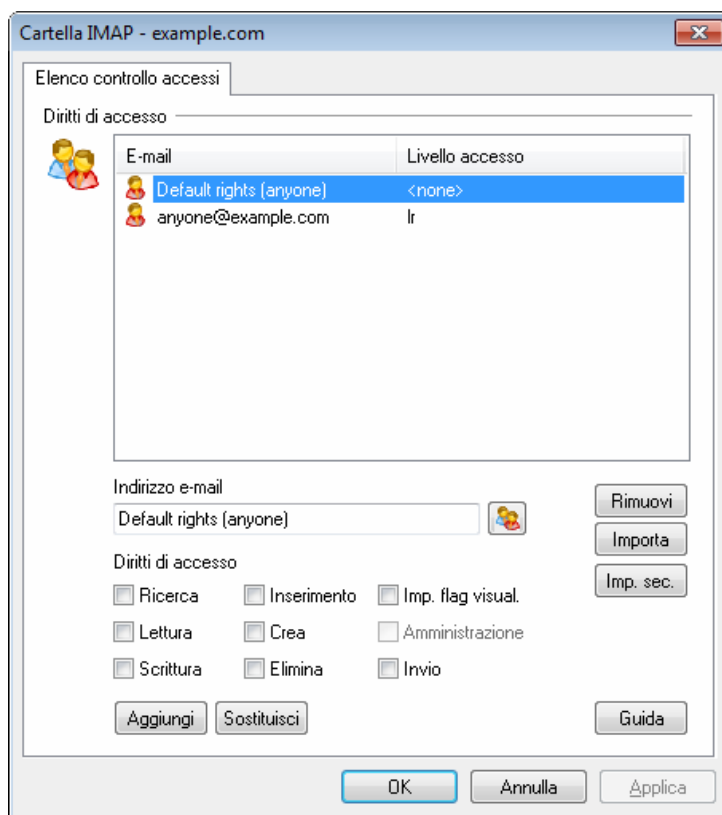
Crea
Una volta specificati il nome di una cartella e altre impostazioni, fare clic su questo pulsante per aggiungere la cartella all'elenco.

Sostituisci
Per modificare una delle voci, selezionarla, apportare le modifiche desiderate in *Nome cartella* o in altre impostazioni e fare clic su *Sostituisci.*

Modifica elenco controllo accessi
Selezionare una cartella e fare clic su questo pulsante per aprire la finestra di dialogo Elenco controllo accessi 80 per la cartella. Utilizzare la finestra di dialogo Elenco controllo accessi per specificare gli utenti o i gruppi a cui sarà consentito accedere alla cartella, nonché le rispettive autorizzazioni.

Vedere:

Elenco controllo accessi 80
Cartelle pubbliche e condivise 76
Account Editor » Cartelle condivise 369

4.1.11.2.1 Elenco controllo accessi

Diritti di accesso

In quest'area è possibile specificare gli account utente o i gruppi di MDaemon a cui si desidera accordare l'accesso alla cartella condivisa associata e impostare le relative autorizzazioni di accesso. Questa finestra di dialogo è raggiungibile dalla schermata Elenco cartelle facendo clic su "Impostazioni » Dominio predefinito/server » cartelle pubbliche e condivise » Elenco cartelle e ACL". Per aprire la finestra di dialogo Elenco controllo accessi relativa a una cartella, fare doppio clic sulla cartella desiderata oppure selezionarla e successivamente fare clic su *Modifica elenco controllo accessi*. Ogni voce visualizza l'indirizzo e-mail dell'account e l'abbreviazione (composta da una lettera) del livello di accesso per ciascun diritto di accesso accordato all'utente.

Indirizzo e-mail

Digitare l'indirizzo e-mail oppure selezionare l'icona Account per selezionare l'account o il gruppo al quale si desidera accordare l'accesso alla cartella condivisa. Dopo aver indicato un account o un gruppo, selezionare i diritti di accesso desiderati e scegliere *Aggiungi* per aggiungere la voce all'elenco.

Rimuovi

Per rimuovere una voce dall'elenco dei diritti di accesso, selezionarla e fare clic sul pulsante *Rimuovi*.

Importa

La funzione *Importa* consente di aggiungere i membri di una lista di distribuzione già esistente all'elenco degli utenti con diritti di accesso. Scegliere i diritti di accesso che si desidera accordare agli utenti, fare clic su Importa, quindi fare doppio clic sulla lista desiderata. Tutti i membri della lista vengono aggiunti all'elenco con i diritti impostati.

Imp. sec.

Fare clic su *Imp. sec.* per applicare le autorizzazioni di controllo accessi della cartella a tutte le sue sottocartelle.

Diritti di accesso

Scegliere i diritti che si desidera accordare ai singoli utenti facendo clic sulle opzioni desiderate in quest'area, quindi fare clic su *Aggiungi* per le nuove voci o su *Sostituisci* per quelle esistenti.

È possibile accordare i diritti di controllo dell'accesso seguenti:

Ricerca (l) - L'utente è in grado di visualizzare la cartella nel proprio elenco personale di cartelle IMAP.

Lettura (r) - L'utente è in grado di aprire la cartella e visualizzarne il contenuto.

Scrittura (w) - L'utente è in grado di modificare i flag applicati ai messaggi della cartella.

Inserimento (i) - L'utente è in grado di allegare e copiare i messaggi nella cartella.

Creazione (c) - L'utente è in grado di creare delle sottocartelle della cartella.

Eliminazione (d) - L'utente è in grado di eliminare i messaggi dalla cartella.

Imp. flag. visual. (f) - L'utente è in grado di modificare lo stato letto/non letto dei messaggi presenti nella cartella.

Amministrazione (a) - L'utente è in grado di amministrare l'ACL (Access Control List) relativo alla cartella.

Invio (p) - L'utente è in grado di inviare la posta direttamente alla cartella, se quest'ultima lo consente.

Aggiungi

Dopo aver scelto dall'elenco un indirizzo e-mail o un gruppo e i diritti di accesso che si desidera accordare, fare clic su *Aggiungi* per aggiungere l'account o il gruppo all'elenco.

Sostituisci

Per modificare una voce di diritto di accesso esistente, selezionare la voce e apportare le modifiche desiderate al diritto di accesso, quindi fare clic su *Sostituisci*..

Guida

Fare clic su *Guida* per visualizzare un elenco dei diritti di accesso e delle relative

definizioni.

I diritti di accesso vengono controllati mediante le funzioni di supporto ACL (Access Control List) di MDaemon. Queste funzioni sono un'estensione del protocollo Internet Message Access Protocol (IMAP4) che consente di creare un elenco di accesso per ogni cartella di messaggi IMAP disponibile, accordando diritti di accesso a tali cartelle anche agli altri utenti che dispongono di un account sullo stesso server di posta. Se il client e-mail in uso non supporta ACL, è comunque possibile impostare le autorizzazioni mediante i comandi di questa finestra di dialogo.

Il protocollo ACL viene descritto approfonditamente nella RFC 2086, consultabile su Internet all'indirizzo `http://www.rfc-editor.org/rfc/rfc2086.txt`.

Vedere:

Cartelle pubbliche e condivise 76
Elenco cartelle 78

4.1.12 DomainPOP

Per configurare MDaemon in modo che scarichi la posta da una casella postale POP remota e la ridistribuisca agli utenti, è necessario utilizzare Raccolta posta DomainPOP, disponibile in "Impostazioni » Dominio predefinito/server » DomainPOP". Questa funzione utilizza il protocollo POP3 per scaricare la posta presente nella casella POP dell'ISP associata all'ID utente specificato. Una volta raccolti, i messaggi vengono analizzati in base ai parametri impostati in questa finestra, quindi collocati nelle caselle postali degli utenti oppure nella coda postale remota per essere consegnati da MDaemon, come se i messaggi fossero stati recapitati al server mediante le transazioni SMTP convenzionali.

È importante tenere presente che i messaggi memorizzati nelle caselle postali POP e ritirati mediante il protocollo POP3 vengono privati di importanti informazioni di instradamento (la cosiddetta "busta" del messaggio) che di solito accompagnano i messaggi consegnati mediante il protocollo SMTP, che offre funzioni più potenti rispetto a POP. Senza tali informazioni, MDaemon deve "leggere" il messaggio ed esaminarne l'intestazione per tentare di identificare il destinatario originale. Tale procedura non è affidabile al 100%. In genere, le informazioni riportate nelle intestazioni dei messaggi non sono sufficienti per identificare il destinatario. Nonostante la mancanza di informazioni essenziali, ovvero il destinatario, costituisca un fattore sorprendente, è opportuno considerare che il protocollo inizialmente utilizzato per la consegna del messaggio non è il protocollo POP. Con il protocollo SMTP, il contenuto del messaggio risulta irrilevante, poiché è il protocollo stesso che indica al server il destinatario del messaggio durante la transazione postale.

Affinché il ritiro e la consegna POP dei messaggi di posta siano affidabili e coerenti,

MDaemon utilizza una serie di potenti opzioni di elaborazione delle intestazioni. Dopo avere scaricato un messaggio da un'origine POP remota, MDaemon ne analizza tutte le intestazioni pertinenti e genera un insieme di potenziali destinatari. Ogni indirizzo e-mail rilevato nelle intestazioni esaminate viene incluso in questo elenco.

Al termine del processo, l'elenco dei destinatari viene suddiviso in due gruppi, uno locale e uno remoto. Prima di questa suddivisione, inoltre, tutti gli indirizzi analizzati e inseriti nell'elenco dei potenziali destinatari vengono elaborati mediante la funzione di conversione degli alias395. Ogni membro del gruppo locale, composto dagli indirizzi il cui dominio corrisponde al dominio predefinito o a uno dei domini aggiuntivi di MDaemon, riceve una copia del messaggio. L'elaborazione degli indirizzi del gruppo locale viene gestita in base alle impostazioni di questa finestra di dialogo. Le opzioni consentono di ignorare semplicemente questi indirizzi, di inoltrare un elenco riepilogativo al postmaster oppure di accettarli. In quest'ultimo caso, MDaemon consegna di fatto una copia del messaggio al destinatario remoto. In rari casi, viene garantita la consegna dei messaggi ai destinatari remoti.

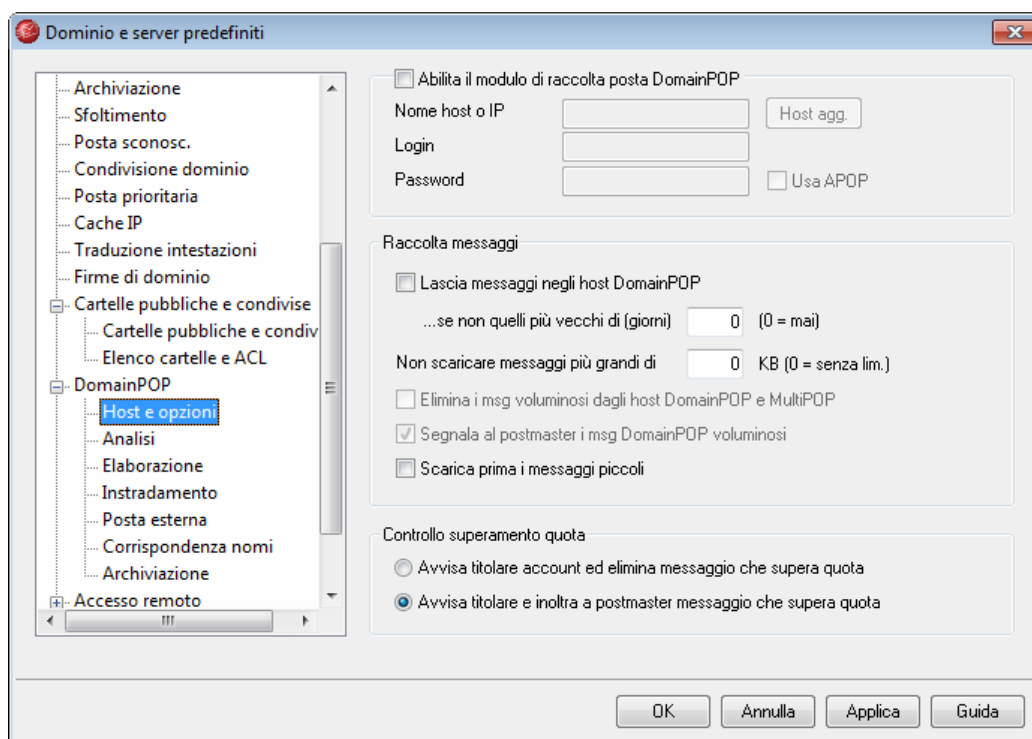
È necessario adottare alcune precauzioni per evitare la duplicazione dei messaggi o un ciclo infinito di consegne. La perdita della busta SMTP, ad esempio, causa un problema nella posta delle liste di distribuzione. Di norma, nel corpo dei messaggi distribuiti da una lista di distribuzione non è presente alcun riferimento all'indirizzo dei destinatari. Il modulo della lista inserisce semplicemente il nome della lista di distribuzione nel campo `TO:`. Questo genera un problema immediato: se nel campo `TO:` è presente il nome della lista di distribuzione, è possibile che MDaemon scarichi il messaggio, analizzi il campo `TO:`, che restituisce il nome della lista, e rispedisca il messaggio alla lista stessa. MDaemon quindi consegnerebbe un'altra copia dello stesso messaggio alla casella postale POP da cui aveva scaricato il messaggio originale, ripetendo lo stesso ciclo all'infinito. Per risolvere problemi di questo tipo, gli amministratori di posta devono essere in grado di utilizzare gli strumenti e le impostazioni di MDaemon per l'eliminazione della posta della lista di distribuzione o per la generazione di alias, così da garantire che i messaggi vengano consegnati ai destinatari locali corretti. Per consegnare correttamente i messaggi, è anche possibile utilizzare le regole di Filtro contenuti o quelle di instradamento.

Questo tipo di raccolta della posta può anche causare una duplicazione indesiderata dei messaggi. È infatti probabile che si generino dei duplicati superflui della posta ritirata mediante DomainPOP e consegnata alla casella postale POP dell'ISP mediante SMTP. Si supponga ad esempio che un messaggio venga inviato a un utente di un dominio di MDaemon e una copia a conoscenza venga inviata a un altro utente dello stesso dominio. In questa situazione, SMTP consegna **due** copie dello stesso messaggio alla casella dell'ISP, una per ogni destinatario. In ognuno dei due messaggi sono presenti i riferimenti a **entrambi** i destinatari: uno nel campo `TO:`, l'altro nel campo `CC:`. MDaemon raccoglierà entrambi questi messaggi identici e analizzerà gli indirizzi riportati in ognuno. In questo modo, ciascuno dei due destinatari riceverà un messaggio duplicato superfluo. Per prevenire questo tipo di duplicazione, in MDaemon è disponibile un comando che consente di specificare un'intestazione che verrà esaminata per la presenza di eventuali duplicazioni. Il campo `Message-ID` (ID messaggio) ha questo preciso scopo. Nell'esempio precedente, entrambi i messaggi sono identici e di conseguenza contengono lo stesso valore nel campo `Message-ID`. Questo valore può essere utilizzato da MDaemon per individuare e rimuovere il secondo messaggio durante la fase di scaricamento, prima di effettuare l'analisi delle informazioni relative all'indirizzo.

Per evitare che i messaggi vengano duplicati e le consegne ripetute all'infinito, è anche possibile monitorare il numero di passaggi (in inglese "hop", salti) effettuati dal messaggio nel sistema di trasporto. A ogni elaborazione, il server di posta SMTP inserisce nel messaggio un'intestazione "Received" per contrassegnarlo come ricevuto. MDaemon conta tutte le intestazioni di questo tipo alla prima elaborazione del messaggio. Se il numero totale di server di posta supera un valore specificato, è probabile che il messaggio sia stato coinvolto in un ciclo di consegne ripetute e che debba essere ritirato dal flusso della posta e collocato nella directory dei messaggi scartati. Tale valore può essere specificato nella schermata Timeout 53 dell'editor del dominio predefinito.

Vedere:

Filtri dei contenuti 211
Liste di distribuzione 428

4.1.12.1 Host e opzioni

Proprietà host DomainPOP

Abilita il modulo di raccolta posta DomainPOP
Se questa casella è selezionata, MDaemon utilizza le impostazioni fornite in questa finestra per raccogliere la posta da un host di posta DomainPOP per poi ridistribuirla a livello locale.

Nome host o IP
Immettere in questo campo il nome dominio o l'indirizzo IP dell'host DomainPOP.

Host agg.
Fare clic su questo pulsante per aprire il file `DpopXtra.dat` nel quale è possibile indicare gli host aggiuntivi utilizzati per la raccolta della posta DomainPOP. Per ulteriori informazioni, vedere il contenuto del file stesso.

Login
Immettere in questo campo l'ID utente dell'account POP utilizzato da DomainPOP.

Password
Immettere in questo campo la password dell'account POP o APOP.

Usa APOP
Selezionare questa casella per utilizzare il comando APOP e l'autenticazione CRAM-MD5 durante il ritiro della posta. Questo comando consente di autenticarsi senza inviare password in testo non crittografato.

Raccolta messaggi

Lascia messaggi negli host DomainPOP
Se questa casella è selezionata, MDaemon scaricherà ma non rimuoverà i messaggi dall'host di posta DomainPOP.

...se non quelli più vecchi di (giorni) (0=mai)
Specificare il numero di giorni per cui si desidera conservare i messaggi nell'host DomainPOP prima di eliminarli. Inserire "0" se non si desidera eliminare alcun messaggio.

Alcuni ISP pongono un limite sulla quantità di messaggi che possono essere contenuti nella casella postale.

Non scaricare messaggi più grandi di [XX] KB (0 = senza lim.)
I messaggi di dimensioni uguali o superiori al valore specificato in questo campo non vengono scaricati dall'host di posta DomainPOP. Specificando il valore "0", i messaggi vengono scaricati a prescindere dalla dimensione.

Elimina i msg voluminosi dagli host DomainPOP e MultiPOP
Selezionare questa opzione per eliminare i messaggi che superano la dimensione massima indicata in precedenza. I messaggi vengono semplicemente rimossi dagli host di posta DomainPOP e MultiPOP senza essere scaricati.

Segnala al postmaster i msg DomainPOP voluminosi
Selezionare questa opzione per inviare un avviso al postmaster e segnalare la presenza di un messaggio di grandi dimensioni nella casella postale DomainPOP.

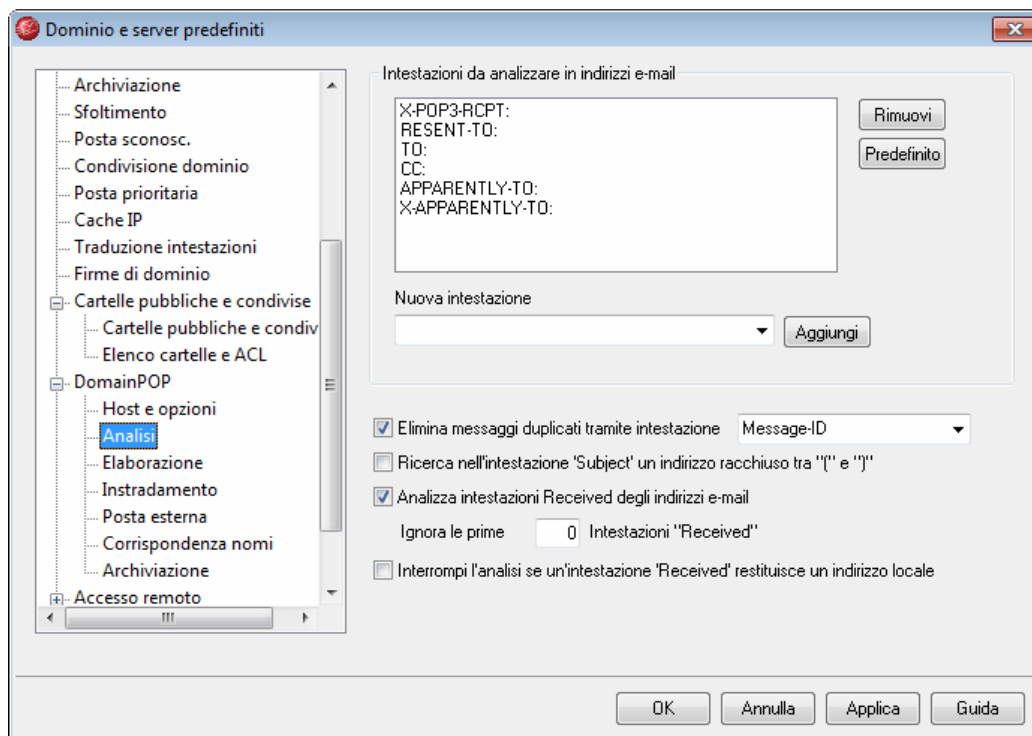
Scarica prima i messaggi piccoli
Selezionare questa casella di controllo per scaricare i messaggi in base alla dimensione, a partire dai più piccoli.

Questa opzione consente di velocizzare il ritiro dei messaggi di dimensione ridotta, ma richiede tempi di ordinamento ed elaborazione interni maggiori.

Controllo superamento quota

Avvisa titolare account ed elimina messaggio che supera quota
Se questa opzione è selezionata e viene raccolto un messaggio per un account il cui valore di quota (specificato nella schermata Quote 364 di Account Editor) è stato superato, MDaemon elimina il messaggio e segnala all'utente che l'account ha superato la quota consentita.

Avvisa titolare e inoltra a postmaster messaggio che supera quota
Se questa opzione è selezionata e viene raccolto un messaggio per un account il cui valore di quota è stato superato, MDaemon inoltra il messaggio al postmaster e segnala all'utente che l'account ha superato la quota consentita.

4.1.12.2 Analisi sintattica

Intestazioni da analizzare in indirizzi e-mail

In quest'area viene fornito l'elenco delle intestazioni analizzate da MDaemon per l'estrazione degli indirizzi. Gli indirizzi vengono cercati in tutte le intestazioni presenti nell'elenco.

Rimuovi
Questo pulsante consente di rimuovere le voci selezionate dall'elenco delle intestazioni.

Predefinito
Questo pulsante consente di cancellare il contenuto corrente dell'elenco delle intestazioni e inserire l'elenco predefinito delle intestazioni di MDaemon. Di solito, le intestazioni predefinite sono sufficienti per estrarre tutti gli indirizzi dal messaggio.

Nuova intestazione
Consente di immettere l'intestazione da aggiungere all'elenco.

Aggiungi
Dopo aver specificato un'intestazione nell'opzione *Nuova intestazione*, per aggiungerla all'elenco fare clic su questo pulsante.

Elimina messaggi duplicati tramite intestazione
Se questa opzione è abilitata, MDaemon memorizza il valore dell'intestazione specificata e non elabora gli altri messaggi con valore identico raccolti durante stesso ciclo di elaborazione. `Message-ID` è l'intestazione predefinita utilizzata per questa opzione.

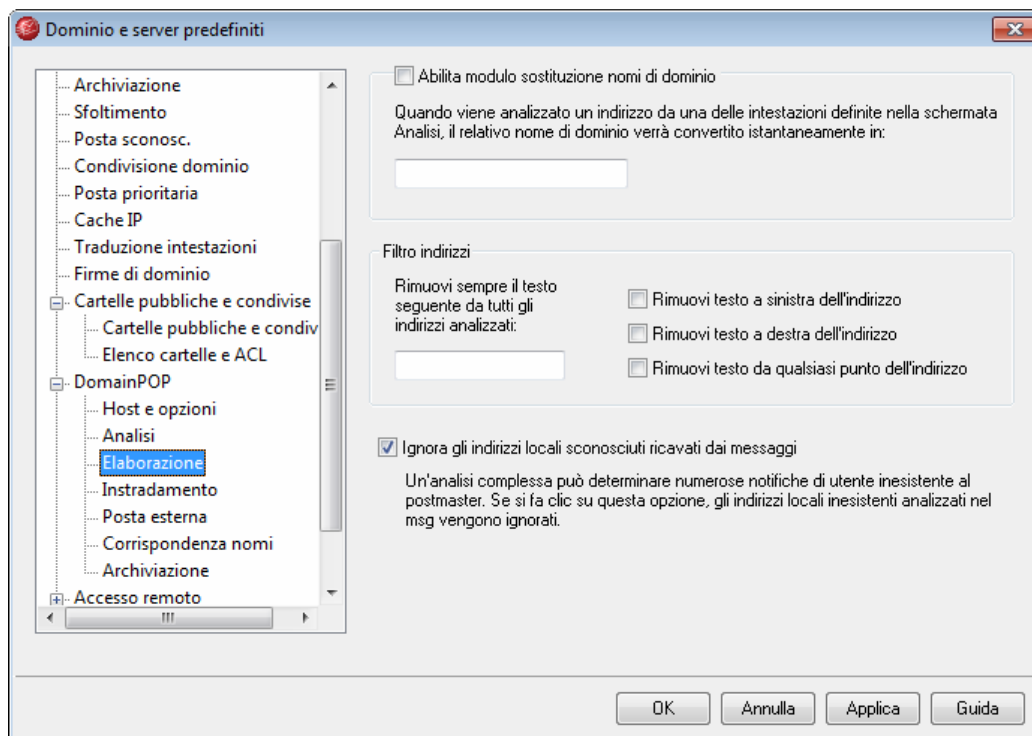
Ricerca nell'intestazione 'Subject' un indirizzo racchiuso tra "(" e ")"
Se questa opzione è abilitata e MDaemon trova un indirizzo racchiuso tra parentesi "( )" nell'intestazione "Subject:" di un messaggio, tale indirizzo viene aggiunto all'elenco dei destinatari del messaggio insieme agli altri indirizzi analizzati.

Analizza intestazioni Received degli indirizzi e-mail
È possibile memorizzare le informazioni relative al destinatario, normalmente presenti solo nelle intestazioni "Received" della busta del messaggio. In questo modo, l'analisi del messaggio rileva l'indirizzo effettivo del destinatario semplicemente esaminando in seguito le intestazioni Received. Selezionare questa casella di controllo per analizzare tutte le intestazioni "Received" trovate nel messaggio al fine di individuare gli indirizzi validi.

Ignora le prime xx intestazioni "Received"
In alcune configurazioni del server, è possibile voler analizzare le intestazioni Received, ma ignorare alcune delle prime. Questa impostazione consente di inserire il numero di intestazioni "Received" che verranno ignorate da MD prima di iniziare l'analisi.

Interrompi analisi se un'intestazione "Received" restituisce un indirizzo locale
Se questa opzione è selezionata e l'analisi sintattica di un'intestazione "Received"

rileva un indirizzo locale valido, MDaemon interromperà il processo di analisi e non cercherà altri potenziali indirizzi di consegna.

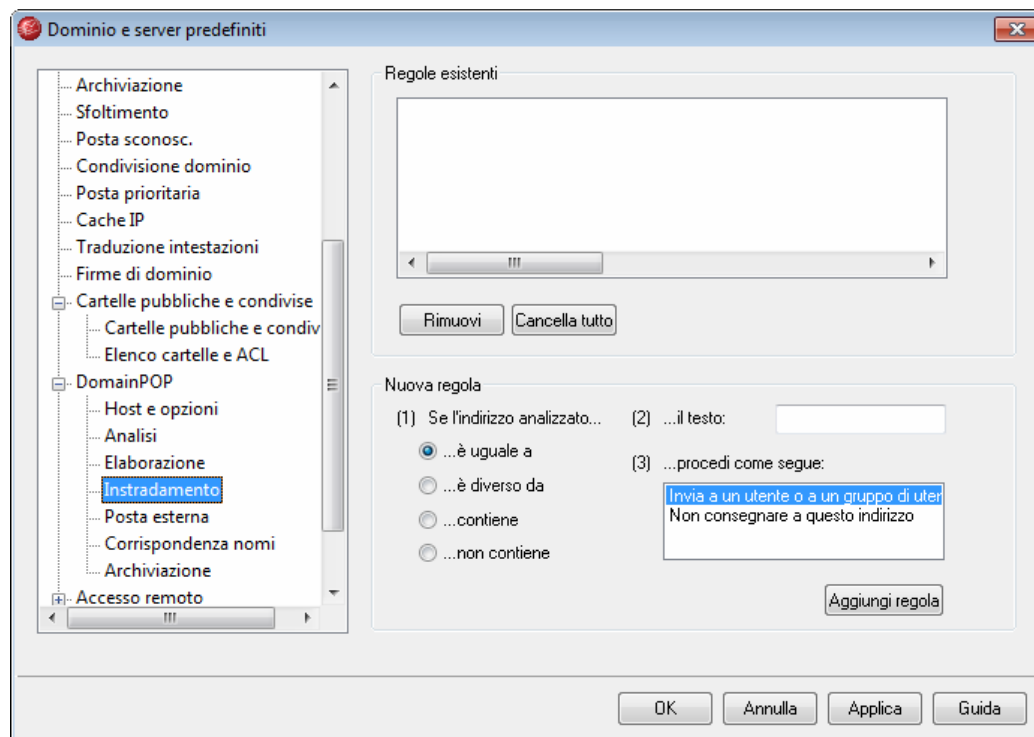
4.1.12.3 Elaborazione

Sostituzione dei nomi di dominio

Abilita modulo sostituzione nomi di dominio
Questa opzione consente di ridurre il numero di alias richiesti dal sito. Quando un messaggio viene scaricato, i nomi di dominio di tutti gli indirizzi analizzati per quel messaggio vengono convertiti nel nome di dominio specificato in questa sede.

Filtro indirizzi

Rimuovi sempre il testo seguente da tutti gli indirizzi analizzati
Alcuni host contrassegnano ogni messaggio con una riga che indica il destinatario del messaggio e aggiungono alcune informazioni sull'instradamento a destra o a sinistra dell'indirizzo. Questo contrassegno costituirebbe lo strumento ideale per analizzare la sintassi dell'indirizzo del destinatario se le informazioni aggiuntive sull'instradamento non rendessero indispensabile un notevole numero di alias per gli account. Per ovviare a questo inconveniente, è possibile specificare semplicemente il valore del testo aggiuntivo nella casella di testo di questa funzione, in modo che MDaemon rimuova ogni occorrenza del testo dagli indirizzi analizzati.

Ignora gli indirizzi locali sconosciuti ricavati dai messaggi
Come indicato in precedenza, la funzione di sostituzione dei nomi di dominio modifica il nome dominio in tutti gli indirizzi e-mail analizzati nel messaggio, sostituendolo con quello specificato in questa finestra. Di conseguenza, è possibile che ad alcuni indirizzi non corrisponda alcun account presso il server. Poiché il nome di dominio è valido, ma la casella postale no, MDaemon considera tali indirizzi come appartenenti a utenti locali sconosciuti. In questi casi, viene generato normalmente il messaggio "Utente inesistente". Abilitare questa casella se si desidera impedire che il modulo di sostituzione dei nomi di dominio generi questi messaggi.

4.1.12.4 Instradamento

Regole esistenti

In questo elenco vengono visualizzate le regole create in precedenza che verranno applicate ai messaggi.

Rimuovi
Per eliminare una regola, selezionarla nell'elenco e fare clic su questo pulsante.

Cancella tutto
Questo pulsante consente di rimuovere tutte le regole esistenti.

Nuova regola

(1) Se l'indirizzo analizzato...

è uguale a, è diverso da, contiene, non contiene
Questi pulsanti di opzione indicano il tipo di confronto che verrà effettuato tra l'indirizzo e la regola di instradamento. MDaemon cerca in ogni indirizzo la stringa specificata nel campo "*il testo*" e procede in base all'impostazione di questo comando. In altri termini, si comporta differentemente a seconda se il testo completo dell'indirizzo corrisponda esattamente, non corrisponda esattamente, includa o non includa il testo specificato.

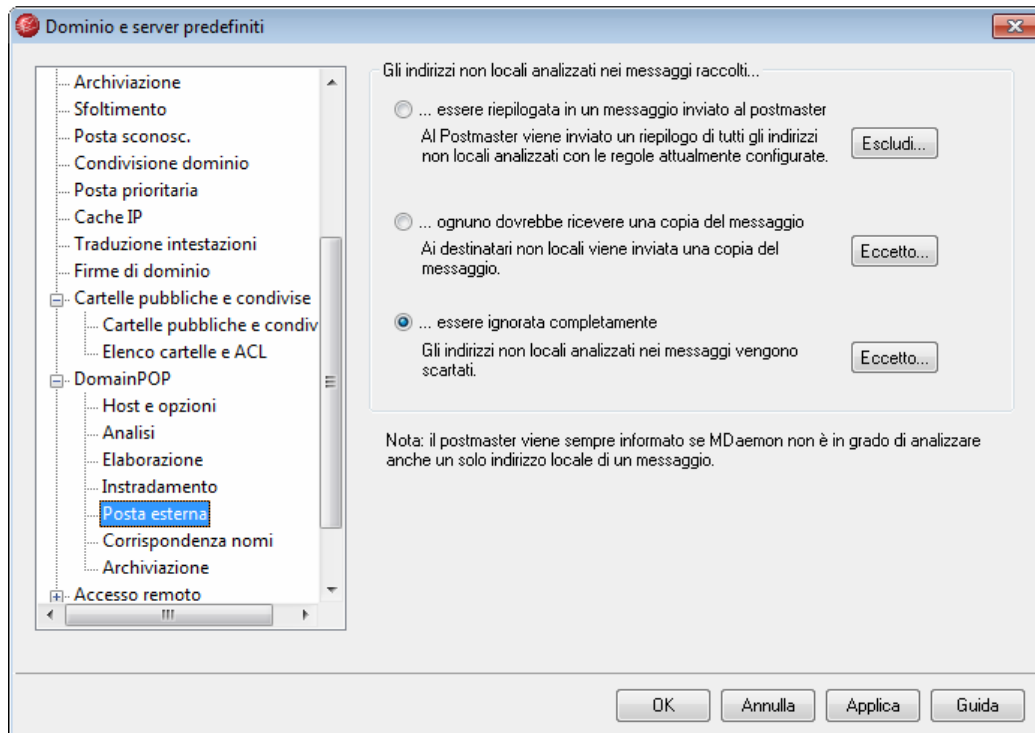
(2) ...il testo:
Immettere il testo da ricercare durante la scansione degli indirizzi.

(3) ...procedi come segue:
In questa casella vengono elencate le azioni che è possibile eseguire quando l'esito della regola è positivo. È possibile scegliere una delle azioni seguenti:

Non consegnare a questo indirizzo - Questa regola impedisce la consegna del messaggio all'indirizzo specificato.

Invia a un utente o a un gruppo di utenti - Questa azione apre una finestra di dialogo che consente di creare l'elenco degli indirizzi e-mail a cui deve essere inviata una copia del messaggio in corso di elaborazione.

Aggiungi regola
Dopo aver impostato i parametri della nuova regola, fare clic su *Aggiungi regola* per aggiungere la regola all'elenco.

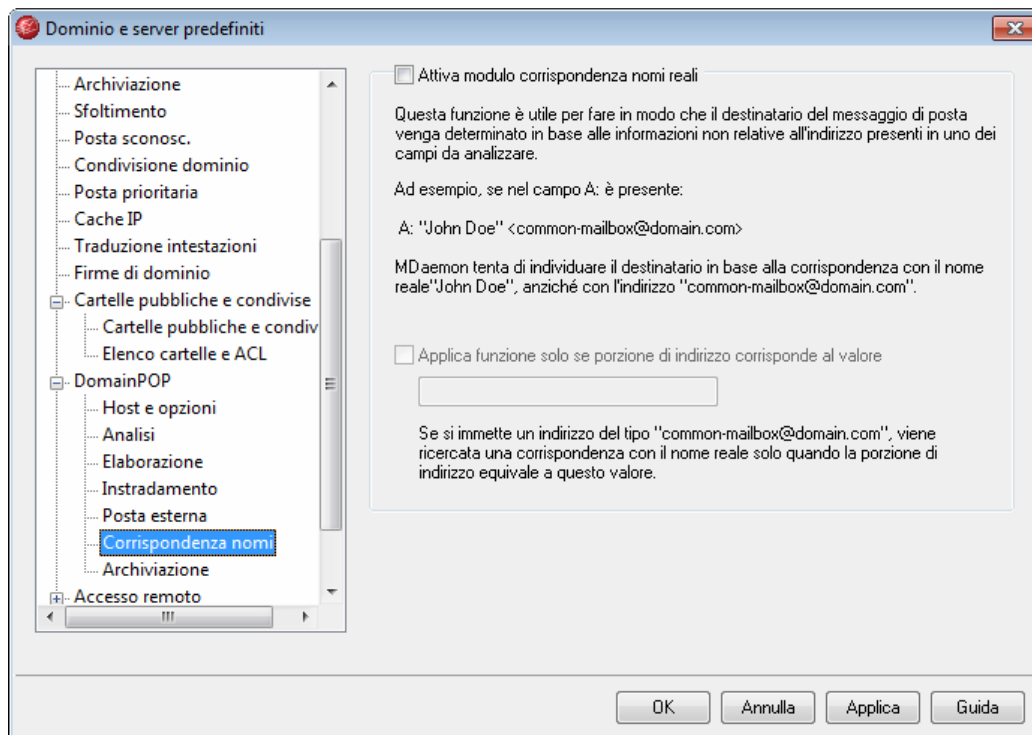
4.1.12.5 Posta esterna

Gli indirizzi non locali analizzati nei messaggi raccolti...

... vengono inclusi in un messaggio inviato al postmaster
Se questa opzione è selezionata, MDaemon invierà al postmaster una singola copia del messaggio insieme a un riepilogo degli indirizzi non locali estratti dall'analisi sintattica mediante la serie corrente di intestazioni e regole.

...ricevono una copia del messaggio
Se questa opzione è selezionata, MDaemon consegna una copia del messaggio ai destinatari non locali eventualmente rilevati nelle intestazioni analizzate.

...vengono ignorati
Se questa opzione è selezionata, MDaemon rimuove dall'elenco dei destinatari tutti gli indirizzi non locali, come se non avesse mai analizzato la sintassi degli indirizzi remoti relativi ai messaggi originali scaricati.

I pulsanti*Escludi* ed *Eccetto* consentono di definire gli indirizzi che rappresentano eccezioni ai fini dell'opzione selezionata.

4.1.12.6 Corrispondenza nomi

La funzione Corrispondenza nomi può essere utilizzata solo insieme al modulo Raccolta posta DomainPOP. Per utilizzare questa funzione, abilitare DomainPOP. Per accedere a DomainPOP, selezionare "Impostazioni » Dominio predefinito/ server » DomainPOP"..

Corrispondenza nomi reali

Attiva modulo corrispondenza nomi reali

Questa funzione consente a MDaemon di individuare il destinatario di un messaggio DomainPOP in base a una porzione di testo inclusa nell'indirizzo anziché all'indirizzo e-mail vero e proprio. In genere, si tratta del nome reale del destinatario.

Si supponga, ad esempio, che un messaggio abbia l'intestazione TO seguente:

```
TO: "Gianni Utente" <casellapostale@esempio.com>
```

oppure

```
TO: Gianni Utente <casellapostale@esempio.com>
```

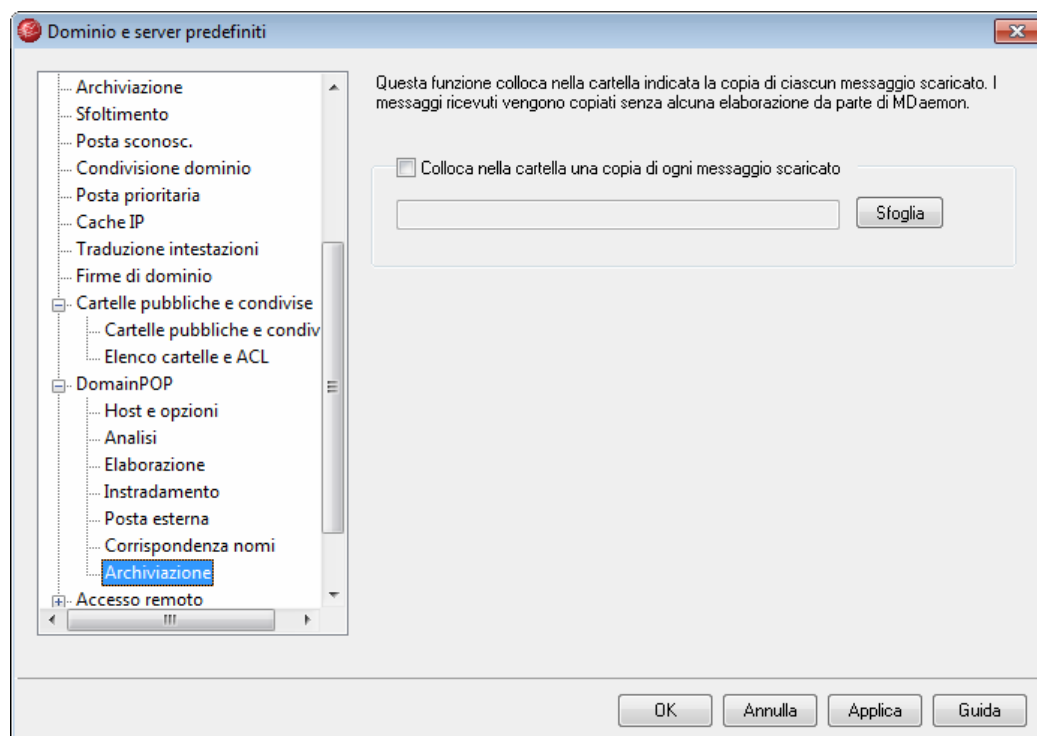
La funzione Corrispondenza nomi ignora la parte "casellapostale@esempio.com" dell'indirizzo, estrae il nome "Gianni Utente" e verifica se tale nome corrisponde a un utente di MDaemon. In caso di corrispondenza con il campo del nome reale di un account, per la consegna verrà utilizzato l'indirizzo e-mail locale di tale account. In

caso contrario, MDaemon consegnerà il messaggio all'indirizzo e-mail determinabile dai dati (in questo caso particolare, "casellapostale@esempio.com").

La parte relativa al nome reale non può includere i caratteri virgola, punto e virgola o due punti.

Applica funzione solo se porzione di indirizzo corrisponde al valore
Questa opzione consente di specificare un indirizzo e-mail che deve essere presente nei dati estratti per avviare il processo di corrispondenza del nome reale. Rappresenta un criterio per determinare quando la funzione Corrispondenza nomi verrà utilizzata. Ad esempio, se l'indirizzo specificato è "casellapostale@esempio.com", la funzione Corrispondenza nomi potrà essere utilizzata solo per gli indirizzi corrispondenti a tale valore.

Se si immette in questo campo il valore "casellapostale@esempio.com", "**`TO: 'Gianni Utente' <casellapostale@esempio.com>`**" è un candidato valido per la corrispondenza dei nomi, mentre "**`TO: 'Gianni Utente' <Gianni@esempio.com>`**" non lo è.

4.1.12.7 Archiviazione

Archiviazione

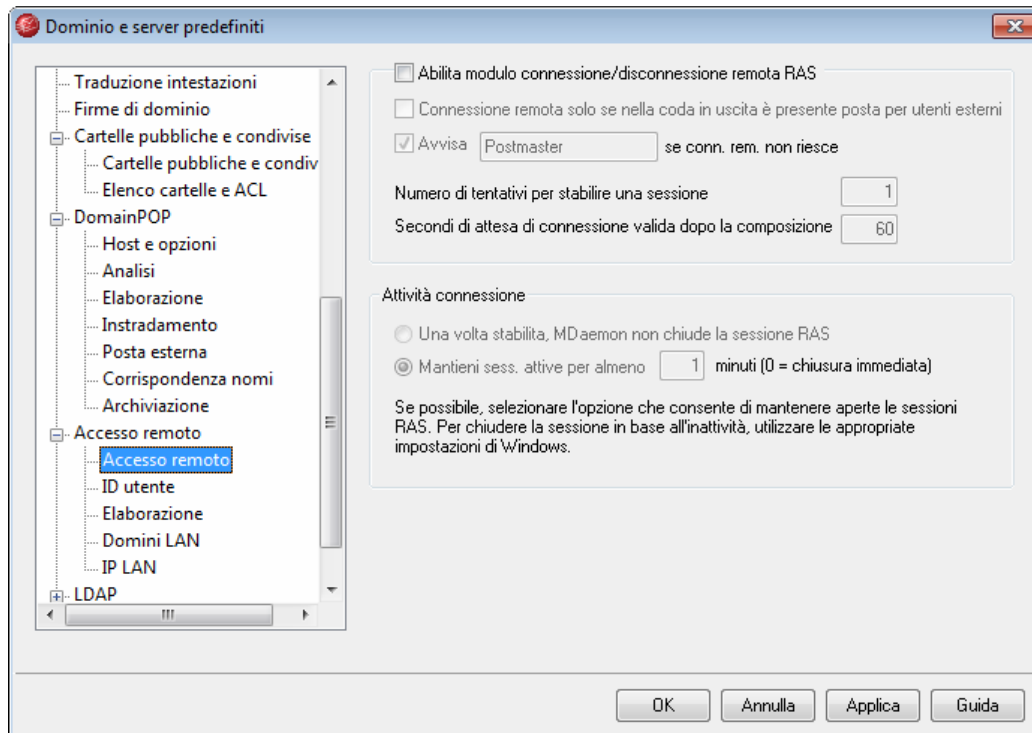
Colloca nella cartella una copia di ogni messaggio scaricato
La selezione di questa opzione impedisce che un'analisi sintattica non prevista o eventuali errori nello scaricamento di notevoli quantitativi di posta causino una perdita di messaggi. Selezionare la casella di controllo se si desidera salvare nella cartella specificata una copia di ciascun messaggio scaricato. Tali copie vengono collocate nella cartella senza alcuna elaborazione da parte di MDaemon.

4.1.13 Impostazioni di connessione remota

Per configurare le impostazioni delle connnessioni mediante accesso remoto, fare clic su "Impostazioni » Dominio predefinito/server » Accesso remoto". Questa finestra è disponibile solo se nel sistema è installato il Servizio di Accesso Remoto (RAS, Remote Access Service), che viene utilizzato da MDaemon per collegarsi all'ISP immediatamente prima di un evento di elaborazione della posta remota.

La finestra Accesso remoto contiene cinque schermate:

- Accesso remoto 95
- ID utente 96
- Elaborazione 98
- Domini LAN 99
- IP LAN 100

4.1.13.1 Accesso remoto

Abilita modulo connessione/disconnessione remota RAS
Se questa opzione è selezionata, MDaemon usa le impostazioni specificate per connettersi a un host remoto prima dell'invio e/o della ricezione della posta remota.

Connessione remota solo se nella coda in uscita è presente posta per utenti esterni
Se questa opzione è selezionata, MDaemon non si connette all'ISP, a meno che nella coda remota non sia presente posta remota in attesa. Nonostante sia vantaggiosa in talune circostanze, tenere presente che se MDaemon non attiva una connessione remota non verrà eseguita neanche la **raccolta** della posta, se non mediante la LAN locale.

Avvisa [indirizzo] se connessione remota non riesce
Se questa casella è selezionata, MDaemon invia un messaggio all'indirizzo specificato per segnalare che la connessione non è riuscita a causa di un errore.

Numero di tentativi per stabilire una sessione
Questo valore indica quante volte MDaemon ha tentato di connettersi all'host remoto prima di abbandonare l'operazione.

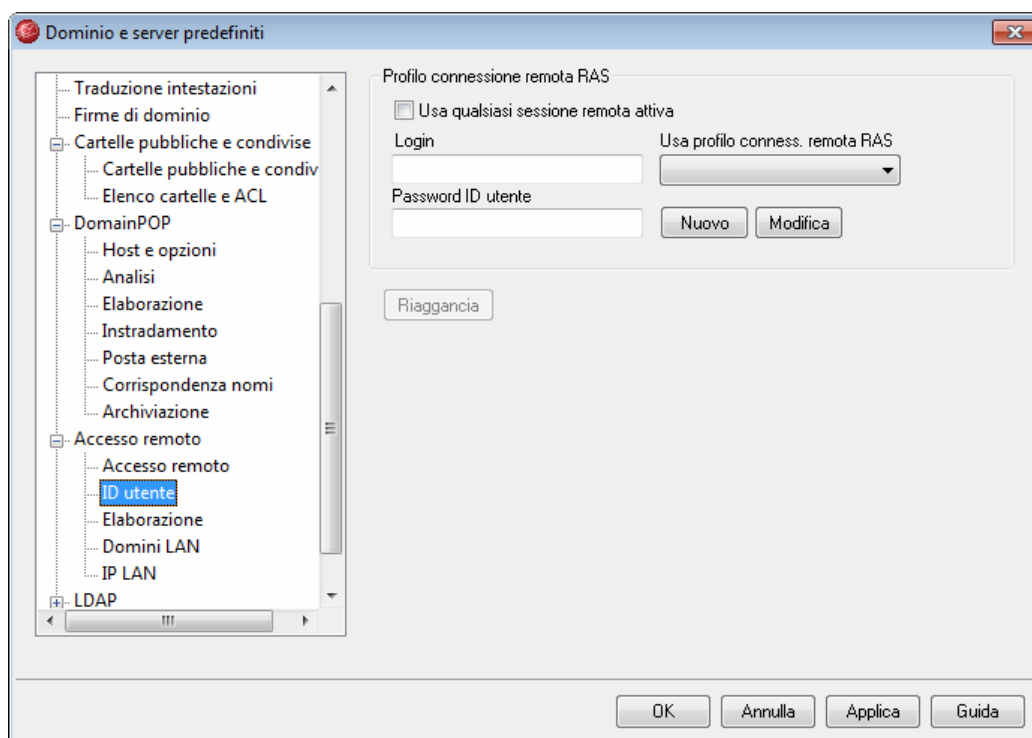
Secondi di attesa di connessione valida dopo la composizione
Questo valore indica il tempo trascorso da MDaemon in attesa della risposta e del completamento della connessione RAS da parte del computer remoto.

Attività connessione

Una volta stabilita, MDaemon non chiude la sessione RAS
Per impostazione predefinita, MDaemon chiude la connessione subito dopo la conclusione di tutte le transazioni postali, quando la sessione non è più utilizzata. Se questa opzione è selezionata, la connessione rimane aperta anche dopo il completamento di tutte le transazioni.

MDaemon non chiude mai una connessione creata da un altro server.

Mantieni sessioni attive per almeno xx minuti
Quando questa opzione è selezionata, una sessione RAS creata da MDaemon rimane aperta per almeno il numero di minuti specificato oppure fino alla conclusione di tutte le transazioni postali, a seconda della situazione.

4.1.13.2 ID utente

Profilo connessione remota RAS

Usa qualsiasi sessione remota attiva
Selezionare questa casella di controllo se si desidera che MDaemon utilizzi altri profili di connessione quando ne rileva uno attivo. Al momento di effettuare la connessione, MDaemon verifica se esiste una connessione attiva prima di stabilirne

una.

Login
Il valore specificato in questo campo viene passato all'host remoto durante il processo di autenticazione.

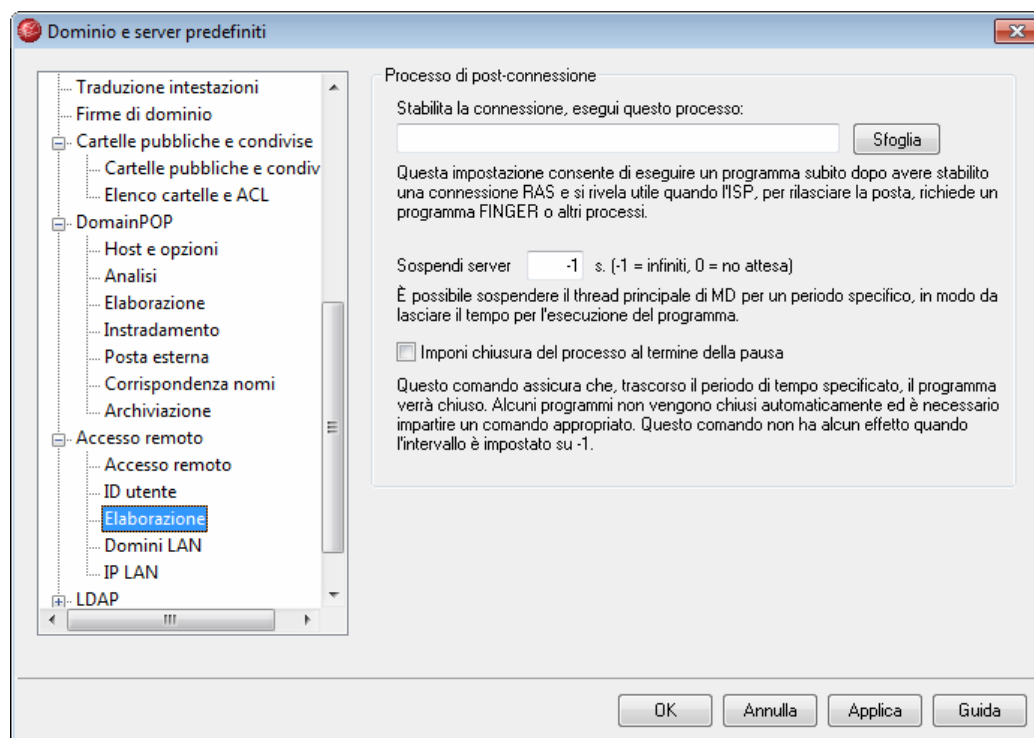
Password ID utente
Il valore specificato in questo campo rappresenta la password trasmessa all'host remoto durante il processo di autenticazione.

Usa profilo connessione remota RAS
In questo elenco a discesa è possibile di selezionare un profilo di sessione definito precedentemente con le opzioni di Accesso remoto di Windows.

Nuovo
Fare clic su questo pulsante per creare un nuovo profilo di accesso remoto o RAS.

Modifica
Fare clic su questo pulsante per modificare il profilo di accesso remoto o RAS correntemente selezionato.

Riaggancia
Se si fa clic su questo pulsante, la connessione all'ISP verrà chiusa. L'opzione è attiva solo se la sessione RAS è stata avviata da MDaemon.

4.1.13.3 Elaborazione

Processo di post-connessione

Stabilita la connessione, esegui questo processo

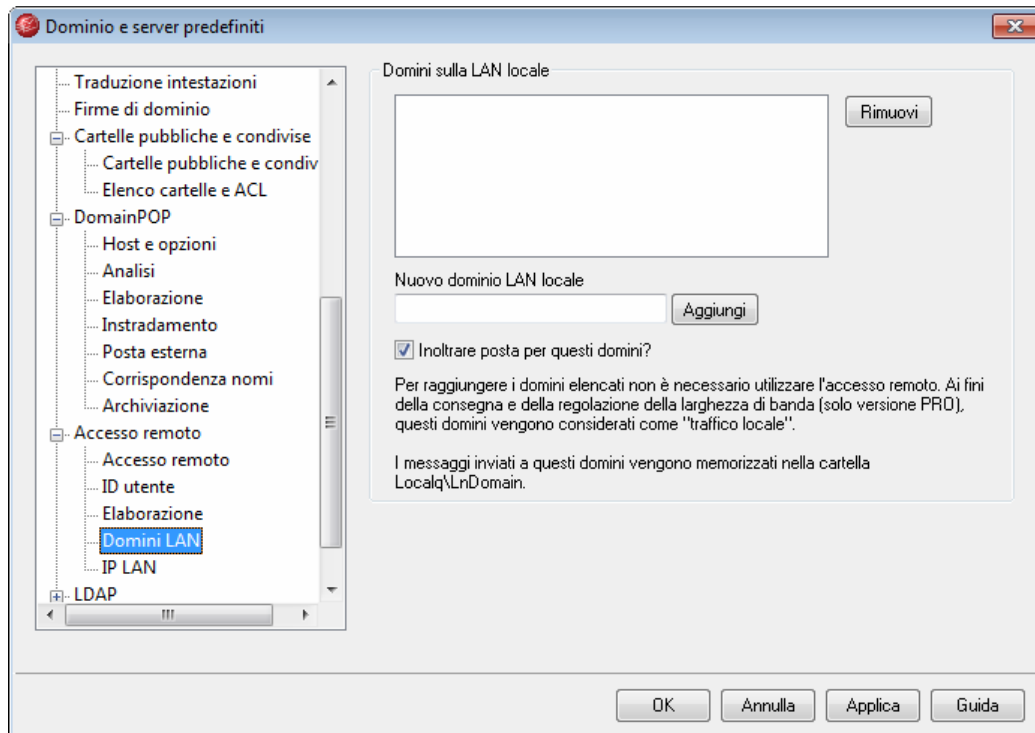
Se in questo campo viene specificato un programma, MDaemon genera un thread ed esegue il processo. Questa funzione è particolarmente utile quando si utilizza `Finger` o un altro programma per sbloccare la casella postale dell'ISP.

Sospendi server xx s. (-1 = infinito, 0 = no attesa)

Se in *Stabilita la connessione, esegui questo processo* è specificata una voce valida, il server sospende le attività per il numero di minuti indicato in questo campo e attende il risultato del processo in esecuzione. Se si immette il valore "-1", il server continuerà ad attendere il risultato del processo.

Imponi chiusura del processo al termine della pausa

In alcuni casi, è possibile che il programma da eseguire non si chiuda automaticamente al completamento: la chiusura di alcuni programmi richiede l'intervento dell'utente. Questa condizione non è accettabile se il software deve essere poter essere eseguito senza la costante supervisione dell'utente. È possibile risolvere il problema selezionando questa opzione per terminare il thread del processo una volta trascorsi i secondi indicati nel campo *Sospendi server XX secondi*. Si noti che la funzione non è attiva se il server è configurato per attendere all'infinito il risultato del processo.

4.1.13.4 Domini LAN

Domini sulla LAN locale

MDaemon considera i domini elencati in questa finestra come parti della LAN locale. Di conseguenza, non è necessaria alcuna connessione per consegnare un messaggio a uno di questi domini.

Nuovo dominio LAN locale

Per inserire un nome di dominio nell'elenco, indicarne il nome e fare clic su *Aggiungi*.

Inoltrare posta per questi domini

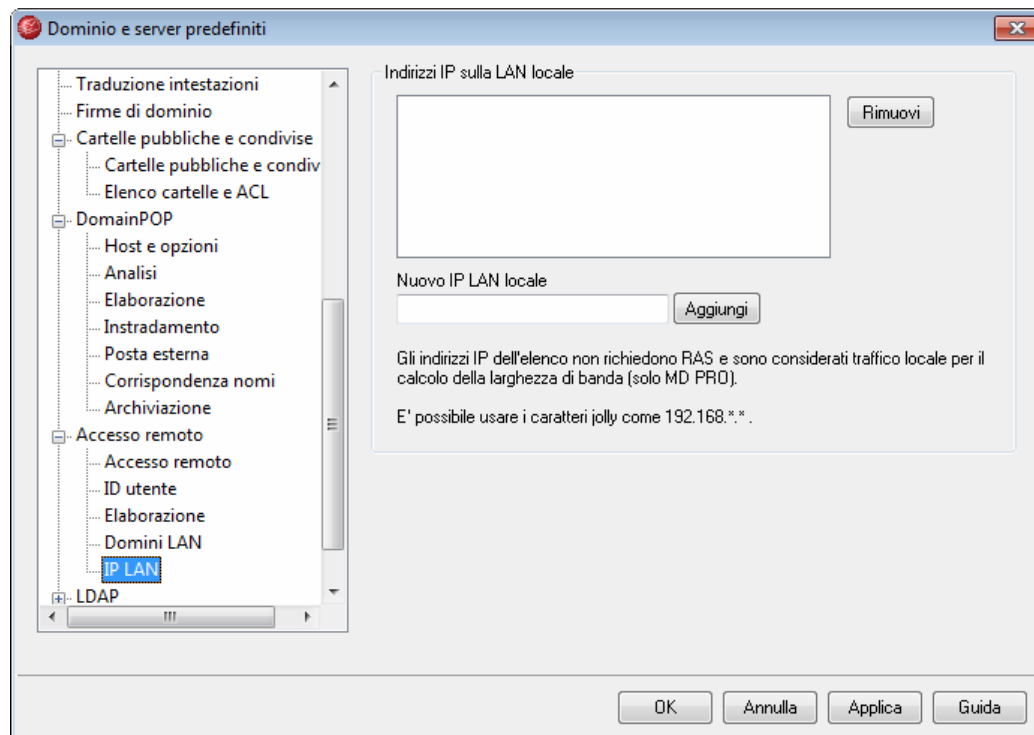
La selezione di questa opzione consente l'inoltro della posta relativa ai domini e offre una forma di controllo sul traffico in entrata e in uscita dai domini.

Aggiungi

Dopo aver specificato un dominio nel campo *Nuovo dominio LAN locale*, fare clic su questo pulsante per aggiungere il dominio all'elenco.

Rimuovi

Selezionare un dominio nell'elenco, quindi fare clic su questo pulsante per rimuoverlo.

4.1.13.5 IP LAN

Indirizzi IP sulla LAN locale

Questa schermata, analoga alla schermata Domini LAN[99], consente di specificare gli indirizzi IP presenti sulla rete LAN locale. Tali indirizzi non richiedono una connessione di accesso remoto e vengono quindi considerati come "traffico locale" ai fini della limitazione della larghezza di banda. Agli indirizzi locali non vengono inoltre applicate numerose limitazioni relative al blocco della posta spam e alla sicurezza.

Rimuovi

Selezionare un indirizzo IP nell'elenco, quindi fare clic su questo pulsante per rimuoverlo. Lo stesso risultato può essere ottenuto facendo doppio clic sulla voce.

Nuovo IP LAN locale

Per aggiungere una voce all'elenco degli IP locali, indicare l'indirizzo IP e fare clic su *Aggiungi*. È possibile utilizzare i caratteri jolly, ad esempio "127.0.*.*".

Aggiungi

Dopo aver immesso un indirizzo IP nel campo *Nuovo IP LAN locale*, fare clic su questo pulsante per aggiungerlo all'elenco.

4.1.14 Opzioni di LDAP e della rubrica

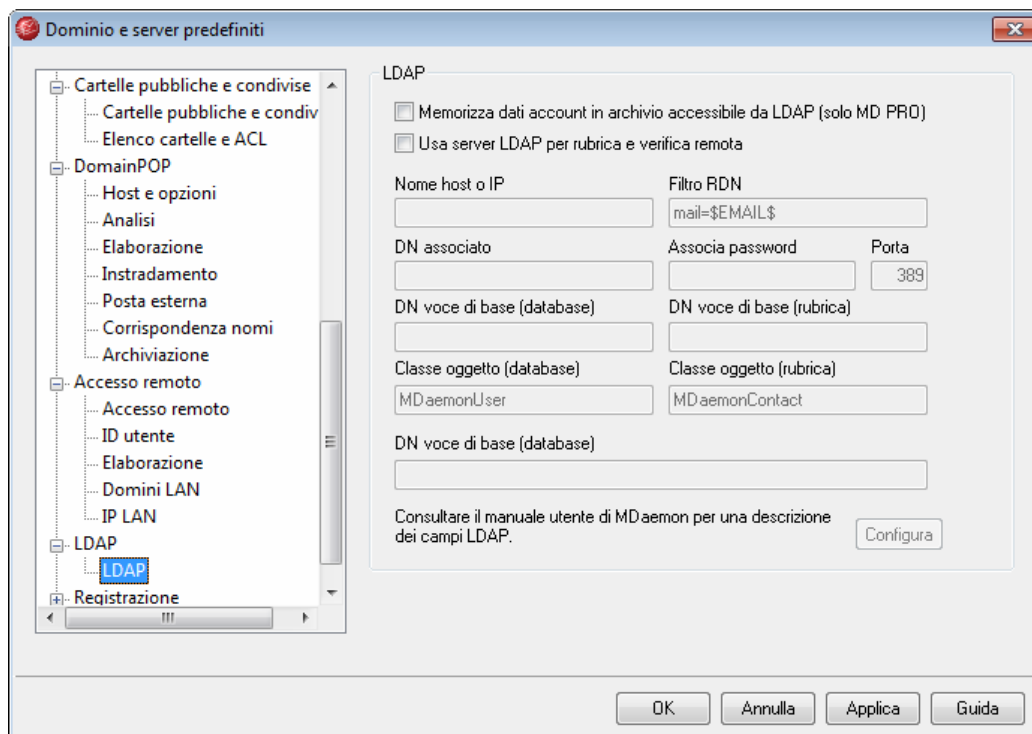
Daemon offre il supporto per il protocollo LDAP (Lightweight Directory Access Protocol). Fare clic su "Impostazioni » Dominio predefinito/server » LDAP" per aprire la

schermata LDAP e configurare MDaemon per l'aggiornamento del server LDAP con tutti gli account utente. MDaemon è in grado di mantenere aggiornato il database degli utenti LDAP comunicando con il server LDAP a ogni aggiunta o rimozione di un account. In questo modo, gli utenti che utilizzano un client di posta che supporta il protocollo LDAP hanno la possibilità di condividere una rubrica globale contenente i contatti di tutti gli utenti di MDaemon e qualsiasi altro contatto desiderato.

È possibile utilizzare il server LDAP come database utenti di MDaemon al posto del sistema `USERLIST.DAT` locale o di un database compatibile con ODBC. Questo metodo di aggiornamento delle informazioni utente può risultare utile se si dispone di più server MDaemon in siti diversi che utilizzano un database utenti condiviso: ciascun server MDaemon viene configurato per connettersi allo stesso server LDAP in modo da condividere le informazioni utente anziché salvarle a livello locale.

Per ulteriori informazioni, vedere:

LDAP 101
Opzioni del database account 408

4.1.14.1 LDAP

LDAP

Memorizza dati account in archivio accessibile da LDAP (solo MD PRO)
Selezionare questa casella di controllo se si desidera che MDaemon utilizzi il server

LDAP come database utenti anziché ODBC o il file USERLIST.DAT locale. Questo metodo di aggiornamento delle informazioni utente può risultare utile se si dispone di più server MDaemon in siti diversi che utilizzano un database utenti condiviso: ciascun server MDaemon viene configurato per connettersi allo stesso server LDAP in modo da condividere le informazioni utente anziché salvarle a livello locale.

Usa server LDAP per rubrica e verifica remota
Se questa opzione è abilitata, è possibile mantenere aggiornati i nomi, gli indirizzi e-mail e gli alias degli utenti del server LDAP sebbene si sia scelto di aggiornare il database account con ODBC o con il metodo predefinito USERLIST.DAT. Di conseguenza, è possibile mantenere aggiornato il server LDAP e utilizzarlo come rubrica globale per i client e-mail che offrono il supporto per le rubriche LDAP.

In tal modo, sarà possibile mantenere un database contenente le caselle di posta, gli alias e le liste di distribuzione che i server di backup remoti possono interrogare per la verifica remota delle informazioni relative all'indirizzo. Per ulteriori informazioni, consultare la successiva sezione *DN della voce di base (verifica remota)*.

Proprietà del server LDAP

Nome host o IP
Immettere in questo campo il nome dell'host o l'indirizzo IP del server LDAP.

Filtro RDN
Questo comando viene utilizzato per generare il nome specifico relativo (o RDN, Relative Distinguished Name) relativo a ciascuna voce LDAP dell'utente. Il nome specifico relativo (RDN) è la porzione all'estrema sinistra del nome specifico (DN) di ogni voce. Poiché per tutte le voci presenti a uno stesso livello (ossia quelle che hanno in comune un livello immediatamente superiore) è necessario un RDN unico, è consigliabile utilizzare l'indirizzo e-mail di ogni utente come RDN in modo da eliminare possibili conflitti. Se come valore dell'attributo specificato in questo comando viene usata la macro $EMAIL$, ossia mail=$EMAIL$), l'attributo viene sostituito dall'indirizzo e-mail dell'utente al momento della creazione della voce LDAP. Il DN dell'utente è costituito dalla componente RDN cui viene aggiunto il valore del campo *DN della voce di base*.

DN associato
Immettere il DN della voce a cui è stato concesso di accedere come amministratore al server LDAP in modo che MDaemon possa aggiungere e modificare le voci relative ai propri utenti. Questo è il DN che viene usato per l'autenticazione nel procedimento di associazione.

Associa password
Nell'autenticazione, questa password viene trasmessa al server LDAP insieme al valore *Associa DN*.

Porta
Specificare la porta monitorata dal server LDAP. Si tratta della porta alla quale MDaemon invia le informazioni sull'account.

DN voce di base (database)
Immettere la voce di base (o DN root) da utilizzare in tutte le voci relative agli utenti di MDaemon quando come database utenti si utilizza il server LDAP anziché il file `USERLIST.DAT`. Per creare il DN dell'utente, il DN della voce di base viene combinato con l'RDN (vedere la precedente sezione *Filtro RDN*).

DN voce di base (rubrica)
Quando si riproducono le informazioni sull'account in una rubrica di database LDAP, immettere la voce di base (o DN root) da utilizzare in tutte le voci relative agli utenti di MDaemon. Per creare il DN dell'utente, il DN della voce di base viene combinato con l'RDN (vedere la precedente sezione *Filtro RDN*).

Classe oggetto (database)
Specificare la classe dell'oggetto a cui deve appartenere ciascuna voce del database utenti dell'utente di MDaemon. In ciascuna voce, al valore presente in questo campo viene associato l'attributo `objectclass=`.

Classe oggetto (rubrica)
Specificare la classe dell'oggetto a cui deve appartenere ciascuna voce di indirizzo LDAP dell'utente di MDaemon. In ciascuna voce, al valore presente in questo campo viene associato l'attributo `objectclass=`.

DN della voce di base (verifica remota)
Un problema diffuso con i gateway di dominio e con i server di backup consiste nel non disporre generalmente di un sistema in grado di stabilire la validità del destinatario del messaggio in entrata. Ad esempio, se al server di backup di esempio.com arriva un messaggio per franco@esempio.com, il server di backup non ha modo di accertare se esista effettivamente una casella postale, un alias o una lista di distribuzione associata a "franco" all'interno di esempio.com, pertanto non può fare altro che accettare tutti i messaggi. MDaemon dispone di un sistema che consente di verificare gli indirizzi risolvendo, così, questo problema. Specificando un DN della voce di base, utilizzato per tutte le caselle postali, gli alias e le liste di distribuzione, il server LDAP è in grado di mantenere aggiornate tutte queste informazioni. In questo modo, ogni volta che arriva un messaggio al dominio, è sufficiente che il server di backup interroghi il server LDAP e verifichi la validità dell'indirizzo del destinatario. In caso negativo, il messaggio viene respinto.

Configura
Fare clic su questo pulsante per aprire il file di configurazione `LDAP.dat` in un editor di testo, utilizzato per specificare i nomi degli attributi LDAP che corrispondono a ciascun campo degli account di MDaemon.

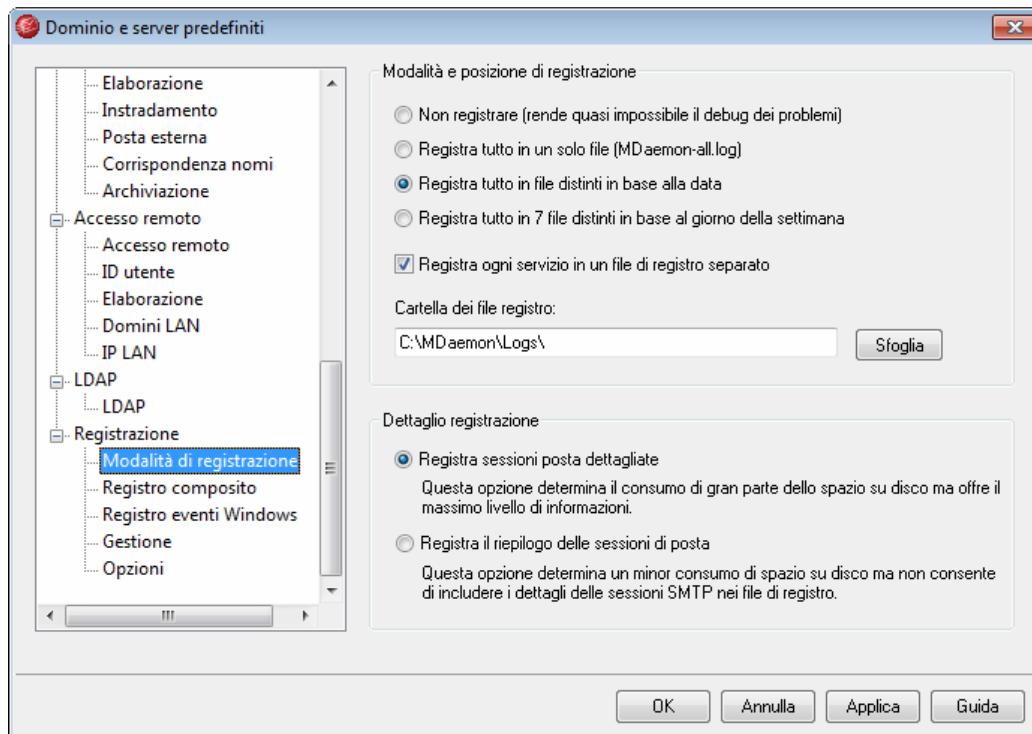
Vedere:

Opzioni del database account 408

4.1.15 Registrazione

Per configurare le impostazioni di registrazione, fare clic su "Impostazioni » Dominio

predefinito/server » Registrazione". La registrazione si rivela utile per la diagnosi dei problemi e il monitoraggio delle operazioni del server durante le attività eseguite senza la supervisione di un utente.

4.1.15.1 Modalità di registrazione

Nella finestra di dialogo Preferenze sono presenti numerosi comandi che consentono di gestire i dati di registro da visualizzare nella finestra Monitoraggio eventi dell'interfaccia principale di MDaemon. Per ulteriori informazioni, vedere Preferenze » GUI 192..

Modalità e posizione di registrazione

Non registrare
Scegliendo questa opzione non verrà attivata alcuna registrazione. Verranno ancora creati i file di registro, ma in essi non verrà scritto alcun dato.

Non è consigliabile utilizzare questa opzione. Senza i registri può risultare estremamente difficile, se non impossibile, eseguire un'analisi o il debug di qualunque eventuale problema legato alla posta.

Registra tutto in un solo file (MDaemon-all.log)
Scegliere questa opzione se si desidera registrate tutte le attività in un unico file

denominato `MDaemon-all.log`.

Registra tutto in file distinti in base alla data
Se questa opzione è selezionata, MDaemon genera un registro separato per ogni giorno. Il nome di ogni file corrisponde alla data di creazione.

Registra tutto in 7 file distinti in base al giorno della settimana
Se questa opzione è selezionata, MDaemon genera un registro separato per ogni giorno della settimana. Il nome di ogni file corrisponde al giorno della settimana in cui è stato creato.

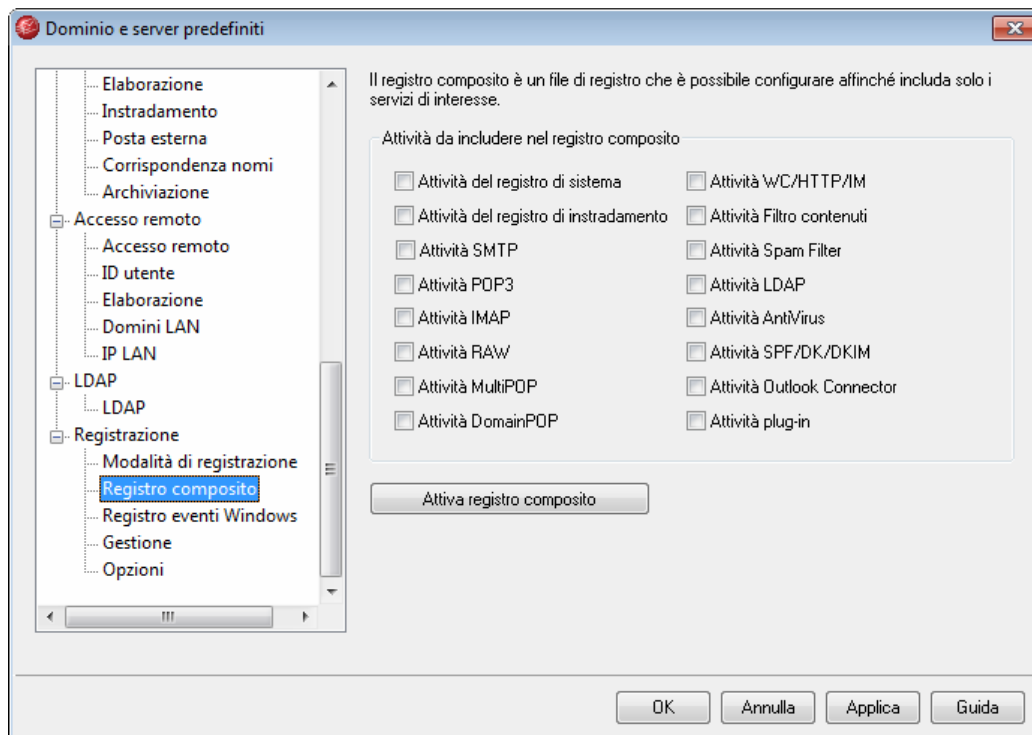
Registra ogni servizio in un file di registro separato
Selezionare questa casella di controllo se si desidera che MDaemon gestisca registri separati per servizio anziché in un unico file. Se si specifica questo comando, ad esempio, MDaemon registrerà l'attività SMTP nel file `MDaemon-SMTP.log` e l'attività IMAP nel file `MDaemon-IMAP.log`. È necessario selezionare questa opzione quando si esegue una sessione di configurazione o un'istanza Servizi terminal di MDaemon, in modo che le informazioni registrate vengano visualizzate nelle schede dell'interfaccia.

Cartella dei file registro:
Utilizzare questa opzione per specificare il percorso della cartella dei file registro.

Dettaglio registrazione

Registra sessioni posta dettagliate
Selezionare questa opzione per copiare nel file registro una trascrizione completa di ogni transazione di posta.

Registra il riepilogo delle sessioni di posta
Selezionare questa opzione per copiare nel file registro un riepilogo di ogni transazione di posta.

4.1.15.2 Registro composito

Registro composito

Attività da includere nel registro composito

L'opzione Vista registro misto è disponibile nel menu Windows della barra dei menu di MDaemon. Facendo clic su questa opzione, nella visualizzazione principale di MDaemon verrà aggiunta una finestra in cui sono riportate informazioni appartenenti a una o più schede di Monitoraggio eventi. Utilizzare i comandi di questa sezione per specificare le schede di cui visualizzare le informazioni nella finestra di visualizzazione del registro composito. È possibile combinare le informazioni provenienti dalle schede seguenti:

Sistema - Attività di sistema, quali l'inizializzazione dei servizi e l'abilitazione/disabilitazione dei vari server di MDaemon.

Instradamento - Informazioni relative all'instradamento (To, From, Message-ID e così via) di ciascun messaggio analizzato da MDaemon.

SMTP - Attività di invio/ricezione delle sessioni che utilizzano il protocollo SMTP.

POP3 - Attività degli utenti che raccolgono la posta elettronica da MDaemon mediante il protocollo POP3.

IMAP - Sessioni di posta in cui è utilizzato il protocollo IMAP.

RAW - Attività di posta RAW o generata dal sistema.

MultiPOP - Attività di raccolta della posta MultiPOP di MDaemon.

DomainPOP - Attività DomainPOP di MDaemon.

WorldClient/HTTP/IM - Attività di WorldClient e attività relativa ai messaggi istantanei di ComAgent.

Filtro contenuti - Operazioni di Filtro contenuti.

Spam Filter - Attività di Spam Filter.

LDAP - Attività LDAP.

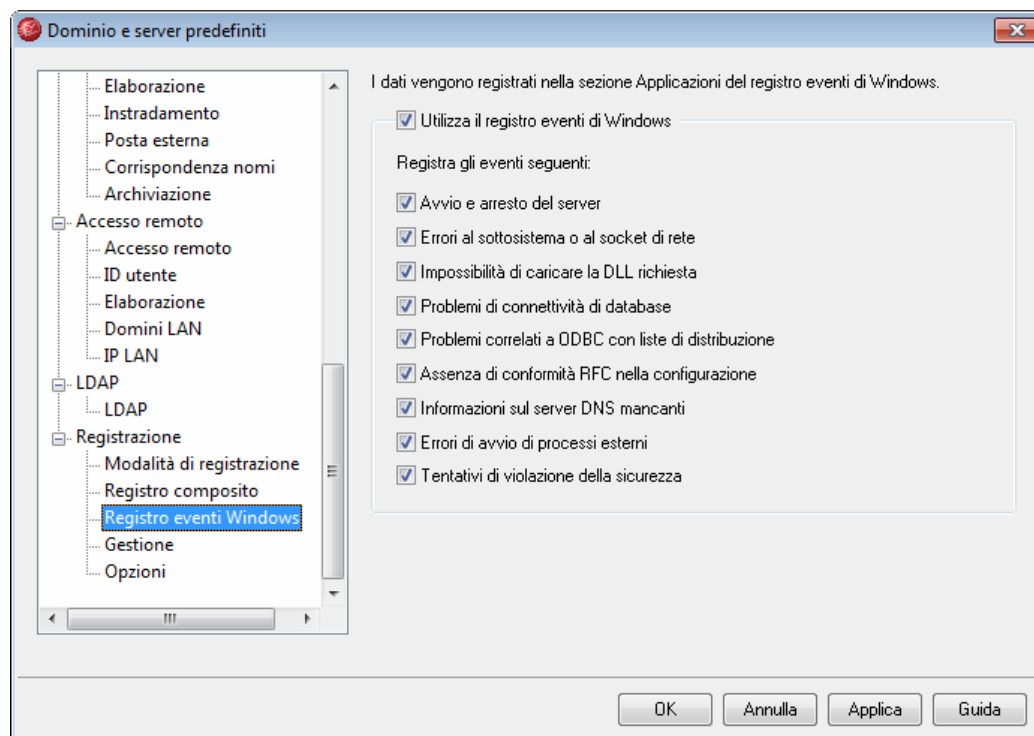
AntiVirus - Operazioni antivirus.

SPF/DK/DKIM - Attività SPF (Sender Policy Framework) e DomainKeys.

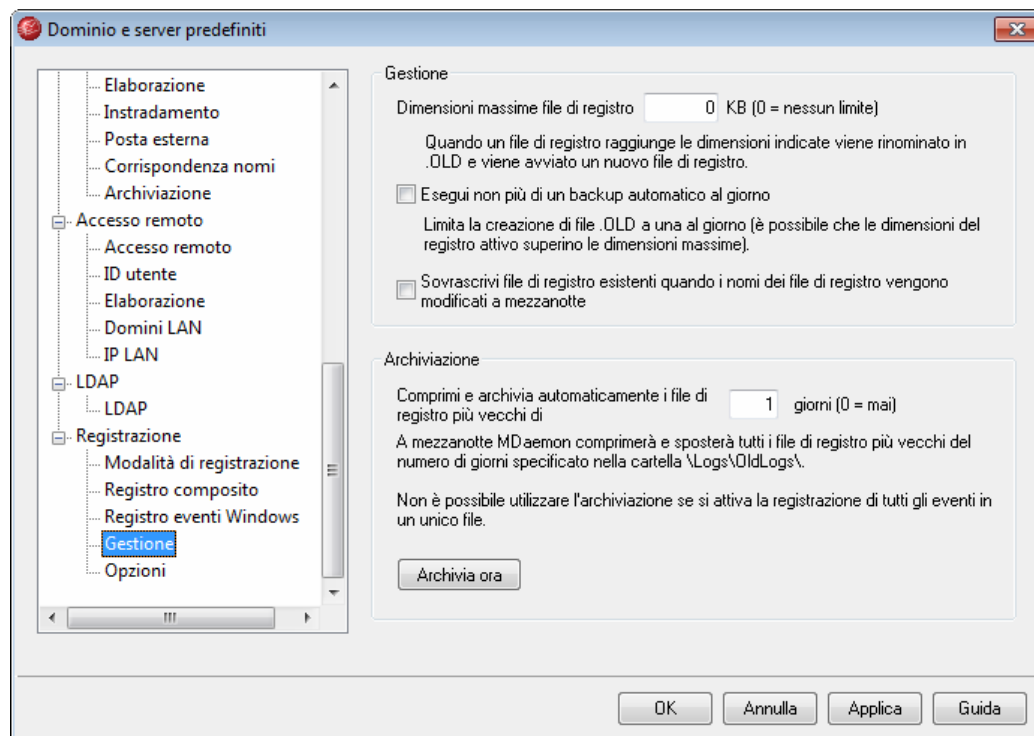
Outlook Connector - Attività di Outlook Connector.

Attività plug-in - Attività dei plug-in di MDaemon.

Attiva registro composito
Selezionare questo pulsante per avviare la finestra del registro composito nella finestra principale di MDaemon. La finestra può essere attivata anche dal menu Finestre della barra dei menu di MDaemon.

4.1.15.3 Registro eventi Windows

Utilizza il registro eventi di Windows
Fare clic su questa casella di controllo se si desidera registrare errori di sistema critici, avvisi e altri eventi nella sezione Applicazioni del registro eventi di Windows.

Registra gli eventi seguenti:
Se si è scelto di registrare gli eventi nel Registro eventi Windows, specificare le caselle di controllo relative al tipo di evento di cui si desidera tenere traccia.

4.1.15.4 Gestione

Gestione

Dimensione max file registro [xx] KB
Indica la dimensione massima in kilobyte consentita per i file registro. Una volta raggiunta tale dimensione, il file di registro viene `copiato` nel file `LOGFILENAME.OLD` e viene creato un nuovo file.

Esegui un solo backup automatico al giorno
Se si pone un limite alla dimensione del file registro, fare clic su questa casella di controllo per generarne un solo backup al giorno. Ogni giorno, non appena viene raggiunta la dimensione massima consentita per il file registro, quest'ultimo viene salvato con l'estensione "`OLD`". La dimensione del file registro continua a crescere a prescindere dalla dimensione massima specificata. Il backup di questo file viene eseguito il giorno successivo, anche se viene superata la dimensione massima.

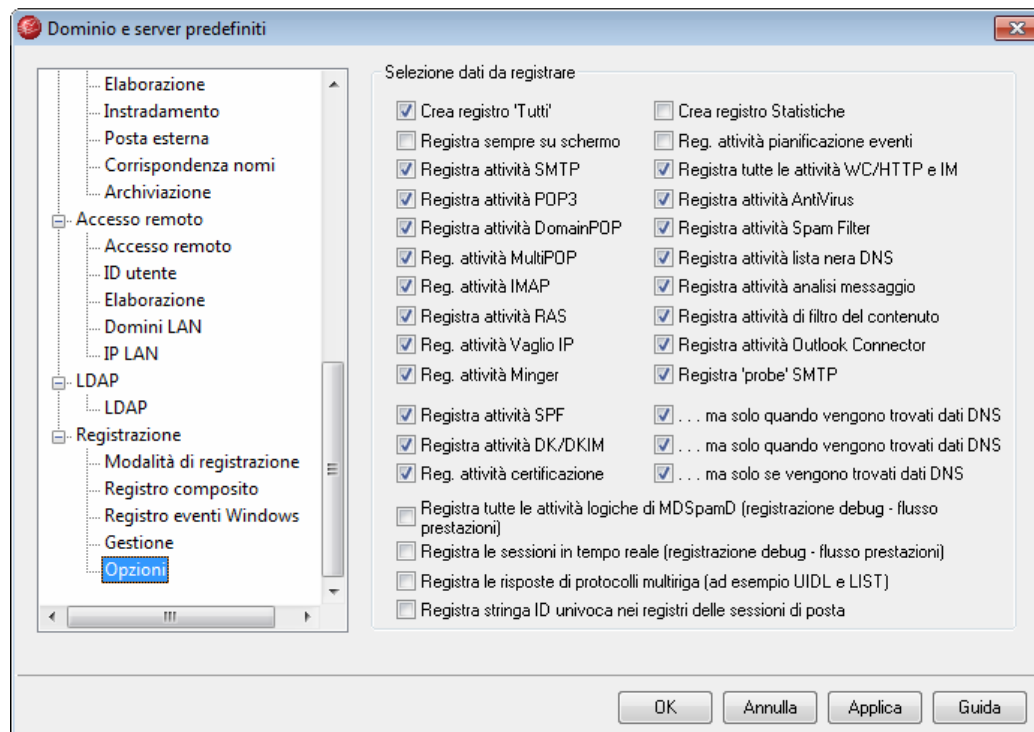
Sovrascrivi file di registro esistenti quando i nomi dei file di registro vengono modificati a mezzanotte
Per impostazione predefinita, quando a mezzanotte modifica il nome dei file registro e il nuovo nome già esiste, MDaemon aggiunge le informazioni appena registrate al

file esistente. Ad esempio, se MDaemon modifica Sabato.log in Domenica.log e già esiste un file denominato Domenica.log, anziché sovrascriverlo o creare un nuovo file, MDaemon aggiunge i dati appena registrati al file esistente. Selezionando questa casella di controllo, si indica di sovrascrivere i file, anziché aggiungere i nuovi dati a quelli esistenti.

Archiviazione

Comprimi e archivia automaticamente i file registro più vecchi di XX giorni (0=mai)
Specificare questa opzione per archiviare i file registro che esistono da più giorni di quelli indicati. Quotidianamente, a mezzanotte, MDaemon comprimerà mediante `ZIP` i file con estensione `.log` e `.old` esistenti e li sposterà nella sottocartella `\Logs\OldLogs\`, eliminando i file originali. Da questo processo vengono esclusi i file in uso. Inoltre, se nella schermata Modalità registrazione è selezionata l'opzione "*Crea un set standard di file registro*", i file non verranno archiviati.

Archivia ora
Se si fa clic su questo pulsante, i file registro precedenti verranno archiviati immediatamente anziché a mezzanotte.

4.1.15.5 Opzioni

Opzioni registro

Crea registro 'Tutti'
Selezionare questa opzione per generare il file "`*-all.log`" contenente l'insieme di

tutte le attività registrate.

Registra sempre su schermo
Selezionare questa opzione se si desidera che i dati registrati vengano copiati nell'interfaccia utente di MDaemon anche quando è ridotta a icona o è in esecuzione nella barra delle applicazioni.

Se la casella di controllo è deselezionata, i dati di registrazione non vengono copiati nella finestra Monitoraggio eventi quando MDaemon è in esecuzione nella barra delle applicazioni. Di conseguenza, all'avvio di MDaemon, l'attività più recente non viene riprodotta in alcuna scheda della finestra Monitoraggio eventi alla prima apertura di MDaemon, ma verranno visualizzate le informazioni registrate a partire da quel punto.

Registra attività SMTP
Selezionare questa opzione per registrare tutte le attività SMTP di invio/ricezione di MDaemon.

Registra attività POP3
Selezionare questa casella di controllo per registrare tutte le attività di posta POP, ossia le sessioni di raccolta della posta POP di tutti gli utenti.

Registra attività DomainPOP
Selezionare questa casella di controllo per registrare tutte le attività di posta DomainPOP.

Registra attività MultiPOP
Selezionare questa casella di controllo per registrare tutte le attività di posta MultiPOP degli utenti.

Registra attività IMAP
Selezionare questa opzione per includere le sessioni IMAP degli utenti nei file registro di MDaemon.

Registra attività RAS
Selezionare questa opzione per copiare nel file registro le attività di connessione/disconnessione RAS. Tali informazioni sono utili per la diagnosi dei problemi di connessione remota.

Registra attività Vaglio IP
Selezionare questa casella di controllo per includere le attività Vaglio IP nel file registro di MDaemon.

Registra attività Minger
Selezionare questa casella di controllo per registrare tutte le attività del server Minger.

Crea registro Statistiche
Poiché i file registro delle statistiche occupano una notevole quantità di spazio su disco e sono alquanto dispendiosi in termini di CPU, è possibile utilizzare questa

opzione per verificarne l'effettiva creazione. L'opzione è disattivata per impostazione predefinita.

Reg. attività pianificazione eventi
Selezionare questa casella di controllo per registrare tutte le attività di Pianificazione eventi 156.

Registra tutte le attività WC e HTTP
Selezionare questa casella di controllo per registrare tutte le attività WorldClient e HTTP, nonché le attività IM (Instant Messaging, Messaggistica istantanea) di ComAgent. Se questa opzione è disattivata, i registri WorldClient e HTTP vengono creati, ma includono solo la data e l'ora di avvio e di arresto di WorldClient. Le altre attività WorldClient, HTTP o IM non vengono registrate.

Registra attività AntiVirus
Selezionare questa opzione per registrare le attività di SecurityPlus per MDaemon.

Registra attività Spam Filter
Selezionare questa opzione per registrare le attività Spam Filter

Registra attività lista nera DNS
Questa opzione consente a MDaemon di registrare l'attività di lista nera DNS e offre un agevole riferimento ai siti registrati come liste nere.

Registra attività analisi messaggio
Per determinare i destinatari dei messaggi, MDaemon svolge regolarmente un'intensa attività di analisi sintattica dei messaggi. Selezionare questa casella di controllo per includere tali informazioni nel file registro.

Registra attività filtro contenuti
Selezionare questa casella per includere nel file di registro le attività della funzione Filtro contenuti.

Registra attività Outlook Connector
Tramite questa opzione è possibile scegliere di registrare le attività Outlook Connector.

Registra 'probe' SMTP
Scegliere questa opzione per registrare le sessioni SMTP quando non vengono trasferiti dati di messaggio dal server di invio, ossia nel caso in cui il server di invio non utilizza il comando DATA.

Registra attività SPF
Selezionare questa casella di controllo per registrare le attività di ricerca SPF.

> **...ma solo se vengono trovati dati DNS**
> Specificare questa opzione se si registrano le attività SPF ma si desidera, durante la ricerca DSN, tenere traccia solo delle ricerche SPF con esito positivo anziché registrare ogni singola operazione.

Registra attività DK/DKIM
Selezionare questa opzione se si desidera registrare le attività DomainKeys (DK) e DomainKeys Identified Mail (DKIM).

...ma solo se vengono trovati dati DNS
Specificare questa opzione se si registrano le attività DomainKeys ma si desidera tenere traccia solo delle istanze contenenti dati DNS anziché registrare ogni singola operazione.

Registra attività certificazione
Selezionare questa casella di controllo per registrare tutte le attività di certificazione dei messaggi.

...ma solo quando vengono trovati dati DNS
Se si registra l'attività di certificazione dei messaggi, questa opzione consente di eseguire la registrazione solo dei dati di certificazione individuati durante le ricerche DNS.

Registra attività MDSpamD (registrazione debug - flusso prestazioni)
Selezionare questa opzione per registrare tutte le attività locali di MDSpamD. Vedere l'avviso riportato di seguito.

Registra le sessioni in tempo reale (registrazione debug - flusso prestazioni)
Per ottimizzare le risorse, le informazioni sulla sessione vengono di solito registrate al termine della sessione. Selezionare questa opzione per registrare le attività in tempo reale.

Se si utilizzano una o entrambe le opzioni di registrazione precedenti, è possibile che le prestazioni del sistema di posta risultino ridotte, in base al computer in uso e al livello di attività. In genere, è opportuno utilizzare queste opzioni solo a scopo di debug.

Registra le risposte di protocolli multiriga (ad esempio UIDL e LIST)
Le risposte alle richieste di protocollo possono occupare più righe. Specificare questa casella di controllo per registrare anche le righe aggiuntive.

Se si seleziona questa opzione, è possibile che la quantità di informazioni registrate aumenti eccessivamente. Poiché non è possibile determinare in anticipo il numero di righe di una risposta e poiché alcune risposte rischiano di "riempire" il file registro con informazioni superflue (ad esempio, POP TOP riproduce il contenuto vero e proprio del messaggio), si sconsiglia l'uso di questa funzione se la dimensione del file registro o la lunghezza del report costituisce un fattore limitante.

Registra stringa ID univoca nei registri delle sessioni di posta
Selezionare questa casella di controllo per includere stringhe di identificazione univoca `[%d:%d]` nelle registrazioni delle sessioni di posta.

4.2 Domini aggiuntivi

4.2.1 Hosting di domini multipli (solo per MDaemon PRO)

MDaemon include il supporto completo dei domini multipli. Oltre alle impostazioni del dominio predefinito 40, include l'Editor dei domini aggiuntivi 115 che consente di indicare tutti i domini aggiuntivi desiderati, nonché gli indirizzi IP associati a ciascuno di essi. MDaemon supporta indirizzi IP sia singoli che multipli.

Per il supporto della funzione multihome (condivisione dello stesso IP da parte di domini diversi), MDaemon rileva automaticamente l'indirizzo IP ricercato dalla connessione in arrivo e utilizza il nome di dominio appropriato. Di seguito è riportato un esempio di configurazione di domini e account.

```
altn.com, IP = 1.1.1.1
utente-1@altn.com, logon = utente-1, password = ALTN

arvelh.com - 2.2.2.2
utente-2@arvelh.com, logon = utente-2, password = ARVELH
```

Ai tentativi di connessione a 1.1.1.1, MDaemon risponde come "altn.com". Per le connessioni a 2.2.2.2, viene utilizzato "arvelh.com".

Quando `utente-1@altn.com` si connette a `1.1.1.1` per controllare la propria casella postale, accede fornendo "`utente-1`" come ID utente e "`ALTN`" come password. Tuttavia, se `utente-2@arvelh.com` si connette a `1.1.1.1` per controllare la propria casella postale, a livello tecnico contatta il server sbagliato (il server corretto dovrebbe essere `2.2.2.2`). In questo caso, per ottenere l'accesso deve indicare il proprio indirizzo e-mail completo nel campo riservato all'ID utente. Naturalmente, se si fosse collegato a `2.2.2.2`, avrebbe dovuto indicare solo il proprio ID utente. Di conseguenza, se un account si connette all'indirizzo IP corrispondente al proprio dominio e tale indirizzo IP non è usato da nessun altro dominio, l'account deve specificare solo il valore dell'ID utente. In caso contrario, è necessario specificare un indirizzo e-mail completo. Questo metodo consente di servire domini multipli usando un solo indirizzo IP. Quando più domini condividono lo stesso indirizzo IP, l'ID utente deve contenere l'indirizzo e-mail completo. In caso contrario, MDaemon non è in grado di riconoscere l'utente che sta cercando di collegarsi. In caso di dubbio, utilizzare l'indirizzo e-mail completo come valore dell'ID utente.

Per un chiarimento su come specificare ID utente e dominio, tenere presenti le considerazioni che seguono. Indicando l'indirizzo e-mail dell'account ci si aspetterebbe di ottenere il seguente risultato: `arvel@altn.com`. MDaemon accetta sempre valori di ID utente contenenti il simbolo '@'. Pertanto se il client di posta supporta l'utilizzo del simbolo '@' nel valore dell'ID utente non si verificherà alcun problema. Alcuni client di posta, tuttavia, non consentono di inserire il simbolo '@' nel campo riservato all'ID utente. Per gestire tali client di posta, MDaemon permette di specificare un carattere

alternativo. Il carattere alternativo predefinito di MDaemon è '$'. È quindi possibile utilizzare sia `arvel$altn.com` sia `arvel@altn.com`.

È possibile indicare il carattere alternativo nella schermata Sistema 194 di Preferenze. Questo valore può essere al massimo di 10 caratteri e consente quindi di utilizzare una stringa di caratteri come delimitatore anziché un carattere singolo, quale '$'. Ad esempio, l'utilizzo di '**.at.**' consente di creare l'ID utente "`arvel.at.altn.com`".

Alcune funzioni essenziali, quali Account, Liste di distribuzione e Impostazioni sicurezza, vengono utilizzate a livello di singolo dominio. Quando si crea un account di posta, occorre specificare il dominio di appartenenza del nuovo account, analogamente alle liste di distribuzione. Di conseguenza alcune funzioni, ad esempio Vaglio IP e Scudo IP, sono legate al singolo dominio mentre altre, ad esempio Corrispondenza nomi 92 di DomainPOP 82, sono legate esclusivamente al dominio predefinito.

Per supportare la gestione dei messaggi di sistema di MDaemon, esiste un set di alias 395 predefiniti che punta a numerosi nomi di caselle postali riservate al nome di dominio predefinito di MDaemon, anziché a singoli domini aggiuntivi:

```
MDaemon@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
listserv@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
listserver@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
list-serv@$LOCALDOMAIN$ = MDaemon@DefaultDomain.com
```

4.2.2 Domini aggiuntivi

Aggiunta di domini

Per aggiungere un altro dominio all'elenco:

1. Fare clic su "Impostazioni » Domini aggiuntivi"
2. Inserire il *Nome dominio*, l'*FQDN* che è spesso coincide con il nome del dominio e l'*indirizzo IP*.
3. Fare clic su *Associa i socket in ascolto all'IP*, **solo** se si desidera associare il dominio al relativo indirizzo IP.
4. Apportare le modifiche desiderate alle altre opzioni.
5. Fare clic su *Aggiungi*.

Modifica di domini aggiuntivi

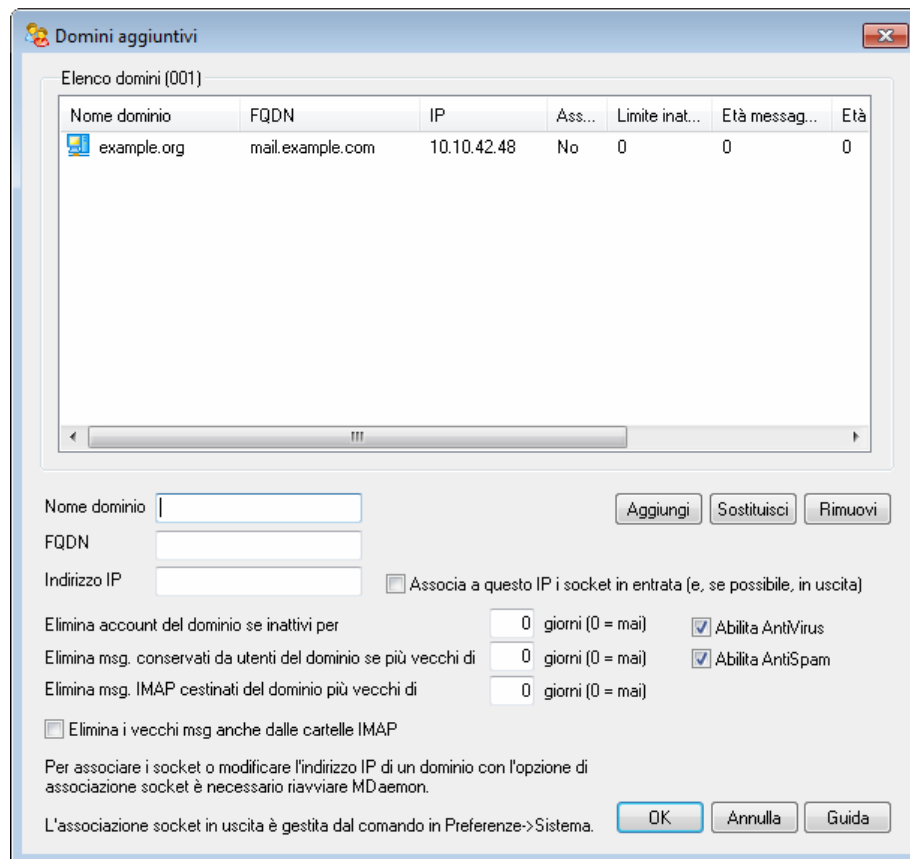
Per modificare un dominio aggiuntivo:

1. Fare clic su "Impostazioni » Domini aggiuntivi"
2. Fare clic sulla voce dell'elenco dei domini che si desidera modificare.
3. Apportare le modifiche desiderate alle altre opzioni.
4. Fare clic su *Sostituisci*.

Rimozione di domini aggiuntivi

Per rimuovere un dominio aggiuntivo:

1. Fare clic su "Impostazioni » Domini aggiuntivi"
2. Fare clic sulla voce dell'elenco dei domini che si desidera rimuovere.
3. Fare clic su *Rimuovi*.

4.2.2.1 Editor dei domini aggiuntivi

Elenco domini

In questa finestra è visualizzato l'elenco dei domini aggiuntivi, suddiviso in diverse colonne: Nome dominio, in cui è riportato il nome di ciascun dominio; IP, in cui viene indicato l'indirizzo IP di ciascun dominio e Associa, che indica se il dominio specifico è associato al proprio indirizzo IP. Le altre colonne corrispondono ai comandi descritti nell'elenco sottostante. L'elenco può essere disposto in ordine crescente o decrescente in base a qualsiasi colonna: fare clic sulla colonna in base a cui si desidera ordinare l'elenco per disporlo in ordine crescente e fare nuovamente clic sulla colonna per disporlo in ordine decrescente.

Nome dominio
Immettere il nome del dominio aggiuntivo di cui si desidera effettuare l'hosting.

FQDN
Questo valore rappresenta il nome di dominio completo (FQDN, Fully Qualified Domain Name) utilizzato nell'istruzione `SMTP HELO/EHLO` al momento di inviare la posta relativa al dominio. Nel caso di connessioni in entrata, se viene utilizzata l'opzione *Associa i socket in ascolto all'IP*, il dominio è associato al proprio indirizzo IP e, per le connessioni effettuate al dominio, viene utilizzato il valore FQDN appropriato. Per garantire il funzionamento, l'opzione "*Associa...*" non è indispensabile, ma se sono disponibili due o più domini che utilizzano lo stesso indirizzo IP in uscita, il valore FQDN utilizzato sarà quello associato al primo dominio in ordine alfabetico.

Nella maggior parte dei casi, il valore FQDN corrisponde al *Nome dominio* indicato in precedenza o a un suo sottodominio, ad esempio "`posta.esempio.com`", ma è possibile utilizzare anche la sintassi letterale IP, ad esempio "`[1.2.3.4]`". Se non si specifica il valore FQDN, MDaemon utilizza il valore FQDN del dominio predefinito.

Indirizzo IP
Immettere l'indirizzo IP da associare al dominio aggiunto o modificato.

Associa a questo IP i socket in entrata (e, se possibile, in uscita)
Selezionare questa casella di controllo per associare il dominio aggiuntivo al relativo indirizzo IP. L'associazione ai socket in uscita è determinata da un'opzione di "Preferenze » Sistema194."

Aggiungi
Fare clic su questo pulsante per aggiungere all'elenco dei domini il dominio aggiuntivo, il relativo indirizzo IP e lo stato di associazione.

Sostituisci
Selezionando una voce nell'elenco dei domini, le relative impostazioni vengono visualizzate nei campi corrispondenti. Se si modificano tali impostazioni, fare clic su questo pulsante per sostituire i valori esistenti con i nuovi valori inseriti.

Rimuovi
Per rimuovere una voce dall'elenco dei domini, selezionarla e fare clic su questo pulsante.

Eliminazione account e messaggi vecchi

Alle quattro opzioni descritte di seguito corrispondono altrettante opzioni di Account Editor364 che possono essere utilizzate al fine di modificare queste impostazioni predefinite per account specifici.

Elimina account del dominio se inattivi per XX giorni (0 = mai)
Consente di specificare per quanti giorni un account del dominio può rimanere inattivo prima di essere eliminato. Specificando il valore "0", gli account non vengono mai eliminati per inattività.

Elimina msg. conservati da utenti del dominio se più vecchi di XX giorni (0 = mai)
Il valore di questo comando indica per quanti giorni un messaggio può rimanere nella casella postale di un utente prima di essere eliminato automaticamente. Il valore "0" indica che, anche se di vecchia data, i messaggi non vengono mai eliminati.

Elimina msg. IMAP cestinati del dominio più vecchi di XX giorni (0 = mai))
Utilizzare questo comando per specificare per quanti giorni i messaggi IMAP contrassegnati per l'eliminazione devono rimanere nelle cartelle dell'utente del dominio. I messaggi contrassegnati per l'eliminazione che esistono da più di XX giorni vengono cestinati dalle rispettive caselle postali. Se si immette il valore "0", un messaggio vecchio contrassegnato per l'eliminazione non viene mai eliminato.

Cancellare i vecchi msg dai folder IMAP
Selezionare questa casella di controllo se si desidera applicare il comando per l'eliminazione dei messaggi conservati dagli utenti anche ai messaggi presenti nelle cartelle IMAP. Se questa opzione è disabilitata, i messaggi contenuti nelle cartelle IMAP non vengono eliminati, a prescindere dal periodo di permanenza nelle cartelle in questione.

-

Abilita AntiVirus
Se *SecurityPlus per MDaemon* 211 è installato, attivare questa casella di controllo per applicarne le impostazioni anche al dominio aggiuntivo selezionato.

Abilita AntiSpam
Attivare questa casella di controllo per applicare le impostazioni Spam Filter correnti anche al dominio aggiuntivo selezionato.

Vedere:

Hosting di domini multipli 113

4.3 Web, Sincronizzazione e Servizi IM

4.3.1 WorldClient (posta Web)

4.3.1.1 Panoramica

WorldClient è una soluzione e-mail basata su Web inclusa in MDaemon, progettata per offrire agli utenti funzionalità di client e-mail tramite il browser Web preferito. WorldClient offre tutte le funzioni di un qualsiasi client di posta tradizionale, nonché un prezioso vantaggio aggiuntivo: consente agli utenti di accedere e utilizzare la posta elettronica ovunque e in qualsiasi momento, disponendo di Internet o di una connessione di rete. Poiché, inoltre, tutte le cartelle e-mail, i contatti, i calendari e così via risiedono nel server anziché nel computer locale, gli utenti dispongono di un accesso completo come se si trovassero alla propria scrivania.

WorldClient offre numerosi vantaggi agli amministratori e-mail. Poiché WorldClient non dipende da una workstation, è possibile configurare tutto mediante il server, a

differenza di molte applicazioni client. In tal modo, non è necessario configurare e gestire i singoli client e-mail. È possibile inoltre personalizzare le immagini grafiche e le pagine HTML utilizzate con WorldClient in modo che soddisfino le specifiche esigenze dell'azienda o dei clienti. Inoltre, è possibile risparmiare tempo consentendo agli utenti di conservare le impostazioni del proprio account. In questo modo, l'amministratore di rete può decidere di accordare agli utenti una maggiore o minore responsabilità di gestione.

Infine, oltre ai vantaggi di un client basato sul Web, esistono molte altre funzioni utili per gli utenti, quali: funzionalità e-mail estese, interfaccia lato client disponibile in quasi 30 lingue, rubriche personali e globali, gestione di cartelle e filtri di posta, invio/ricezione di file allegati, numerosi "temi" grafici per l'interfaccia, temi per dispositivi mobili, funzioni di calendario, funzioni GroupWare, un'applicazione di messaggistica istantanea integrata da scaricare e installare sul desktop e molto altro ancora.

Funzioni di calendario e pianificazione

MDaemon è dotato di un sistema di collaborazione completo. È possibile creare appuntamenti, pianificare riunioni e gestire rubriche direttamente da WorldClient. Sono pienamente supportate le funzioni dedicate agli appuntamenti ricorrenti, che possono essere descritti dettagliatamente tramite campi appositi. Inoltre, i contatti, i calendari e i dati sulle attività vengono memorizzati sotto forma di cartelle IMAP nelle directory di posta principali degli utenti. Tramite WorldClient, gli utenti possono accedere a queste cartelle personali e controllare quali altri utenti vi hanno accesso. In tutti i temi di WorldClient, in particolare Lookout, sono disponibili modelli che consentono di presentare le cartelle dei contatti, del calendario, delle note e delle attività in modo più logico e intuitivo.

Grazie all'integrazione del sistema di calendario, è possibile creare notifiche e-mail per appuntamenti, anche pianificati da terze parti. Ogni volta che una terza parte pianifica un appuntamento per l'amministratore, questi riceve un messaggio e-mail di riepilogo. Ciascun partecipante alle riunioni riceve un messaggio e-mail che indica la data, l'ora, il luogo e l'argomento della riunione e fornisce un elenco completo dei partecipanti. Inoltre, se nel calendario di un partecipante è previsto un evento in conflitto con la fascia oraria della riunione, viene inviato un messaggio di avviso per notificare l'impegno e la sovrapposizione di orario. L'organizzatore riceve un messaggio di riepilogo contenente tutti i dettagli della riunione e un elenco dei partecipanti (con e senza conflitti di orario).

Il sistema di calendario è inoltre dotato del supporto per Internet Calendar (iCal), utilizzato da Microsoft Outlook e da altri programmi e-mail compatibili con iCalendar ed è in grado di rilevare ed elaborare le informazioni di iCalendar inviate agli utenti e di utilizzarle per aggiornare i calendari. All'apertura di un allegato iCalendar da WorldClient, le informazioni contenute nell'allegato vengono riprodotte nel calendario WorldClient dell'utente. Inoltre, quando gli utenti creano dei nuovi appuntamenti o delle nuove riunioni, possono specificare uno o più indirizzi e-mail a cui desiderano sia inviato un messaggio e-mail iCalendar. I singoli utenti possono impostare questa funzione nelle opzioni WorldClient.

ComAgent

ComAgent include un sistema di messaggistica istantanea protetto, un client di rubrica e un'applet visualizzata nella barra delle applicazioni che fornisce l'accesso rapido alle

funzioni e-mail di WorldClient. ComAgent può essere scaricato da ogni utente di WorldClient e successivamente installato nei singoli computer locali. Poiché viene preconfigurato per lo specifico utente al momento dello scaricamento, non richiede un livello approfondito di configurazione manuale.

ComAgent, che viene eseguito in background, controlla l'eventuale presenza di nuovi messaggi per l'account interrogando direttamente il server WorldClient. In questo modo, non è più necessario aprire un browser e mantenerlo aperto durante il controllo della posta. ComAgent verifica se sono presenti nuovi messaggi e, in caso affermativo, ne trasmette notifica all'utente con un segnale acustico o visivo. In ComAgent viene inoltre visualizzato un elenco delle cartelle di posta insieme al numero e al tipo di messaggi (nuovi, non letti e letti) contenuti in ognuna. Tra le altre cose, può essere utilizzato per avviare il browser e indirizzarlo immediatamente a una cartella di posta specifica, al primo messaggio non letto, alla pagina di composizione di un messaggio o alla pagina del calendario.

ComAgent offre anche la possibilità di stabilire una sincronizzazione bidirezionale della rubrica tra MDaemon e Outlook o Outlook Express sul computer locale di ciascun utente. Pertanto, anche se si utilizzano Outlook (o Outlook Express) e WorldClient in tempi diversi, le rubriche corrisponderanno.

Infine, ComAgent è dotato di un sistema di messaggistica istantanea completo, che consente di visualizzare l'elenco degli utenti ComAgent con il relativo stato, ad esempio online, disconnesso o assente, nonché di avviare una conversazione con un singolo utente o un gruppo, di impostare il proprio stato online e di visualizzare le conversazioni precedenti in una cartella ordinata cronologicamente.

Per istruzioni più dettagliate, consultare la Guida in linea di ComAgent.

Sistema di messaggistica istantanea di ComAgent

ComAgent è dotato di un semplice ma efficiente sistema di messaggistica istantanea (IM), che consente di comunicare istantaneamente con qualsiasi altro account del server MDaemon. È possibile scegliere un elenco di compagni di conversazione dall'elenco degli utenti di MDaemon e sapere sempre quali sono in linea e pronti per ricevere un messaggio IM. Inoltre, è possibile avviare una conversazione di gruppo con più utenti. Tutte le funzioni IM sono disponibili nel menu di scelta rapida dell'icona nella barra delle applicazioni e nella finestra ComAgent.

Al sistema IM di ComAgent è inoltre possibile applicare gli script, in modo da creare un'interfaccia con eventuali programmi personalizzati. Grazie alla creazione di file semaforo (`SEM`) nella cartella \MDaemon\WorldClient\, un'applicazione esterna è in grado di inviare messaggi IM agli utenti di ComAgent. Di seguito è riportato il formato del file SEM:

`To: franco@esempio.com`	Indirizzo e-mail dell'utente di ComAgent.
`From: ric@esempio.com`	Indirizzo e-mail del mittente del messaggio istantaneo.
`<riga vuota>`	
`Testo del messaggio istantaneo.`	Testo inviato come messaggio istantaneo.

Il nome del file SEM deve iniziare con i caratteri "IM-", seguiti da un valore numerico univoco. Ad esempio, "IM-0001.SEM". Le applicazioni devono creare un file corrispondente denominato "IM-0001.LCK" per bloccare il file SEM. Una volta completato il file SEM, rimuovere il file LCK per avviare l'elaborazione del file SEM. MDaemon utilizza questo metodo di script per inviare dei promemoria IM relativi ad appuntamenti e riunioni imminenti.

Il sistema Filtro contenuti è dotato di un'azione che invia i messaggi istantanei avvalendosi di questo metodo di script. Inoltre, le regole che utilizzano questa azione possono includere nel messaggio istantaneo le macro di Filtro contenuti. È possibile, ad esempio, creare una regola per l'invio di una regola di messaggio istantaneo con righe come quelle riportate di seguito:

```
Messaggio e-mail da $SENDER$.
Subject: $SUBJECT$
```

Questa regola rappresenta un modo efficace per inviare avvisi di nuovi messaggi mediante ComAgent.

Molte aziende e amministratori non si avvalgono pienamente dei sistemi di messaggistica istantanea perché non è consentito gestirli centralmente e non è possibile monitorare il traffico IM nei client IM tradizionali più diffusi. Il sistema di messaggistica istantanea di ComAgent è stato progettato appositamente per minimizzare tali problemi. Innanzitutto, il sistema non è di tipo peer-to-peer: i singoli client ComAgent non si connettono direttamente l'uno all'altro. Inoltre, poiché ogni messaggio IM passa per il server, viene registrato in una posizione centrale accessibile da parte dell'amministratore di MDaemon/WorldClient. In questo modo, è possibile conservare una registrazione di tutte le conversazioni e garantire la sicurezza sia dell'azienda che degli utenti. L'attività IM viene registrata nel file InstantMessaging.log presente nella directory MDaemon\LOGS\. Non vengono supportati altri client, quali ICQ, AOL e MSN, specificamente per garantire la gestione centralizzata. Infine, il sistema IM di ComAgent è protetto: ogni transazione viene crittografata dall'inizio alla fine e le informazioni pertanto non vengono mai trasmesse sotto forma di testo in chiaro.

La funzione di messaggistica istantanea agisce a livello di singolo dominio. I comandi per attivare i messaggi istantanei e specificare l'eventuale registrazione del traffico IM sono disponibili nella schermata ComAgent/IM della finestra di dialogo WorldClient ("Impostazioni » Web, Sincronizzazione e Servizi IM » ComAgent/IM").

Skin di ComAgent

L'interfaccia di ComAgent è compatibile con gli skin *msstyles*, facilmente reperibili via Internet. Comprende numerosi stili, ma per installarne uno nuovo è necessario scaricare il file *.msstyles e inserirlo nella cartella \Styles\ di ComAgent, in una sottocartella che abbia lo stesso nome del file. Se, ad esempio, il file è stato denominato Yoda.msstyles il percorso sarà: "\.\Styles\Yoda\Yoda.msstyles"

Sincronizzazione automatica delle rubriche

Utilizzando ComAgent insieme al sistema di rubrica integrata di MDaemon, è possibile stabilire una sincronizzazione a due vie tra MDaemon e la rubrica di Outlook o Outlook Express su ciascun computer locale. Pertanto, anche se si utilizzano Outlook (o Outlook

Express) e WorldClient in tempi diversi, le rubriche corrisponderanno.

MDaemon gestisce un database utenti dettagliato, che viene aggiornato a ogni aggiunta, rimozione o modifica di un account. ComAgent è in grado di eseguire regolarmente query nel server LDaemon e acquisire tutte le informazioni sui contatti memorizzate. Queste informazioni vengono pubblicate nella Rubrica di Windows o nell'archivio contatti del computer locale. In questo modo, vengono aggiornati istantaneamente tutti gli eventuali pacchetti software che utilizzano il sistema della rubrica, ad esempio Outlook o Outlook Express.

Chiunque utilizzi ComAgent con le opportune credenziali di accesso può aggiungere contatti pubblici utilizzando direttamente la Rubrica di Windows oppure Outlook o Outlook Express. Il nuovo contatto viene prelevato da ComAgent e caricato nella rubrica di MDaemon. Gli altri utenti della rete potranno accedere al nuovo contatto alla successiva query eseguita da ComAgent a MDaemon.

Nella schermata Sincronizzazione della finestra di dialogo Preferenze di ComAgent è possibile specificare le cartelle della Rubrica di Windows con cui si desidera eseguire la sincronizzazione. È possibile indicare cartelle separate sia per i contatti pubblici sia per quelli privati.

La sincronizzazione dei file WAB (Windows Address Book) della Rubrica di Windows richiede IE 5 o superiore e l'abilitazione del supporto per le identità.

Per informazioni sulle altre opzioni della rubrica, vedere:

WorldClient (posta Web) » ComAgent/IM 131
LDAP 101
Rubrica di Windows 415

4.3.1.2 Uso di WorldClient

Avvio di WorldClient

Sono disponibili tre modi per avviare/arrestare il server WorldClient:

1. Nella scheda Statistiche presente nel riquadro sinistro della GUI di MDaemon, fare clic con il pulsante destro del mouse sulla voce WorldClient e scegliere l'opzione *Attiva/Disattiva* dal menu di scelta rapida.
2. Nell'interfaccia principale, fare clic su "File » Abilita server WorldClient".
3. Selezionare "Impostazioni » Web, Sincronizzazione e Servizi IM" nell'interfaccia principale, quindi fare clic su *WorldClient in esecuzione con server Web incorporato* nella schermata Server Web.

Accesso a WorldClient

1. Aprire mediante il browser la pagina `http://esempio.com:NumeroPortaWC`. NumeroPortaWC

viene definito nella schermata Server Web 123 della sezione relativa a WorldClient. Se si configura WorldClient affinché utilizzi la porta Web predefinita (porta 80), non è necessario indicare il numero di porta nell'URL di accesso. In questo caso, è sufficiente specificare `www.esempio.com` anziché `www.esempio.com:3000`.

2. Digitare il nome utente e la password dell'account MDaemon.
3. Fare clic su Entra.

Modifica delle impostazioni della porta di WorldClient

1. Fare clic su "Impostazioni » Web, Sincronizzazione e Servizi IM" nella barra di menu.
2. Digitare il numero della porta desiderata nella casella *Esegui il server WorldClient su questa porta TCP*.
3. Fare clic su OK.

Guida del client

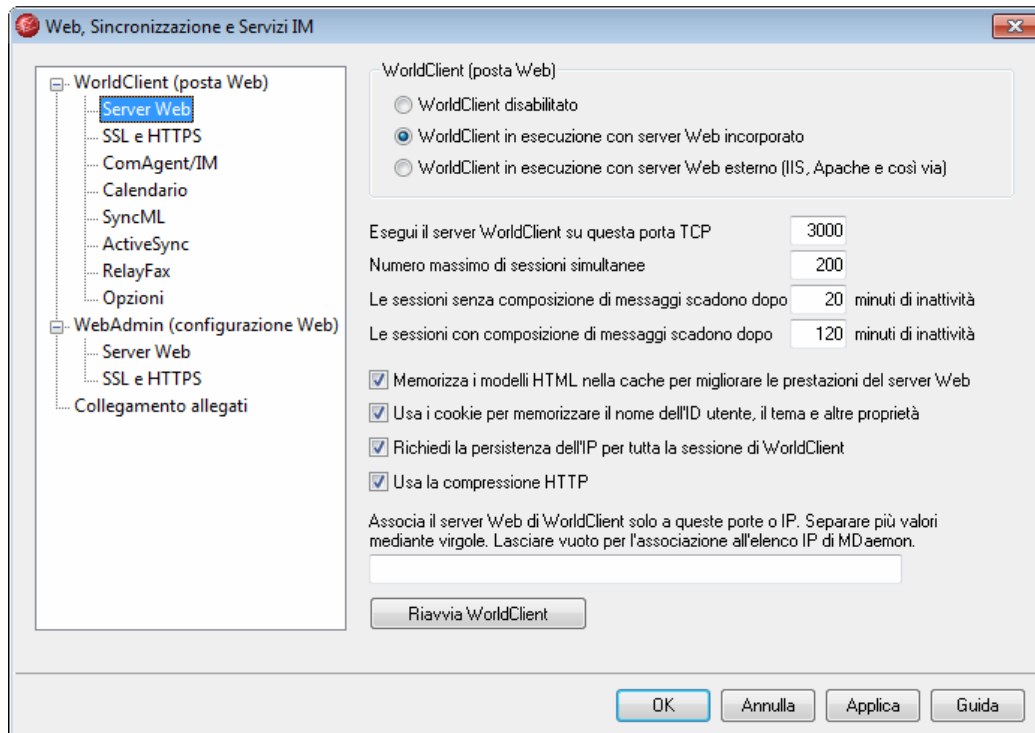
WorldClient viene fornito con una guida completa delle funzioni lato client. Per informazioni sulle funzioni e sulle caratteristiche del client, consultare la Guida in linea di WorldClient.

4.3.1.3 WorldClient (posta Web)

Per abilitare il server WorldClient e configurarne le varie impostazioni, selezionare "Impostazioni » Web, Sincronizzazione e Servizi IM » WorldClient (posta Web)". Le opzioni presenti nella relativa finestra di dialogo consentono di definire la porta da assegnare al server e l'intervallo di tempo di inattività di una sessione di WorldClient prima della scadenza. È inoltre possibile controllare numerose impostazioni globali o relative a uno specifico dominio, ad esempio la lingua e il tema predefiniti, l'autorizzazione alla creazione di account da parte degli utenti, l'impaginazione predefinita dell'elenco dei messaggi, l'abilitazione/disabilitazione del supporto per ComAgent, l'autorizzazione a utilizzare la messaggistica istantanea e la relativa registrazione, la configurazione del supporto di SSL e dei certificati, l'integrazione con RelayFax e molto altro ancora.

Per ulteriori informazioni sulle diverse sezioni di WorldClient, fare clic sui collegamenti seguenti.

Server Web 123
SSL / HTTPS 128
ComAgent/IM 131
Calendario 133
SyncML 135
RelayFax 139
Opzioni 140

4.3.1.3.1 Server Web

In questa schermata sono incluse diverse impostazioni globali a livello di server che consentono di controllare la configurazione e il comportamento di WorldClient, a prescindere dagli utenti o dai relativi domini di appartenenza.

Proprietà di WorldClient

WorldClient disabilitato
Scegliere questa opzione per disabilitare WorldClient. Il server WorldClient può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon.

Per utilizzare la funzione Collegamento allegati 154, è necessario che WorldClient sia attivo.

WorldClient in esecuzione con server Web incorporato
Scegliere questa opzione per eseguire WorldClient utilizzando il server Web incorporato di MDaemon. Il server WorldClient può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon.

WorldClient utilizza server Web esterni (IIS, Apache e così via)
Scegliere questa opzione se si desidera eseguire WorldClient in Internet Information Server (IIS) o in un altro server Web diverso dal server incorporato di MDaemon. In questo modo, è possibile impedire l'accesso a elementi della GUI che potrebbero entrare in conflitto con il server alternativo.

Per ulteriori informazioni, vedere Esecuzione di WebAdmin con IIS 125.

Esegui il server WorldClient su questa porta TCP
Si tratta della porta da cui WorldClient riceve le richieste di connessione provenienti dai browser degli utenti.

Numero massimo di sessioni simultanee
È il numero massimo di sessioni che possono connettersi contemporaneamente a WorldClient.

Le sessioni senza composizione di messaggi scadono dopo xx minuti di inattività
Si tratta dell'intervallo di tempo durante il quale la sessione può rimanere inattiva (un utente ha effettuato l'accesso a WorldClient ma non compone alcun messaggio di posta) prima che WorldClient la chiuda.

Le sessioni con composizione di messaggi scadono dopo xx minuti di inattività
Questo timer stabilisce per quanto tempo la sessione dell'utente rimarrà aperta mentre viene composto il messaggio (e la sessione risulta inattiva). È buona norma impostare il timer su un valore superiore rispetto a quello definito per l'opzione *Le sessioni senza composizione di messaggi...*, in quanto l'intervallo di inattività è normalmente superiore durante la composizione di un messaggio. La composizione di un messaggio non richiede infatti alcun tipo di comunicazione con il server finché il messaggio non viene inviato.

Memorizza i modelli HTML nella cache per migliorare le prestazioni del server Web
Selezionare questa casella di controllo se si desidera che WorldClient memorizzi i modelli nella cache anziché leggerli ogni volta che è necessario accedervi. In questo modo è possibile aumentare sensibilmente le prestazioni del server. Tuttavia, è necessario riavviare WorldClient se si apportano delle modifiche a uno dei file di modello.

Usa i cookie per memorizzare il nome dell'ID utente, il tema e altre proprietà
Selezionare questa opzione se si desidera che WorldClient memorizzi un cookie contenente il nome dell'ID utente, il tema e altre proprietà nel computer locale in uso. Questa funzione consente di offrire agli utenti un accesso più "personalizzato", a condizione che nei loro browser sia abilitato il supporto per i cookie.

Richiedi la persistenza dell'IP per tutta la sessione di WorldClient
Come misura di sicurezza aggiuntiva, è possibile selezionare questa casella di controllo affinché WorldClient limiti ciascuna sessione utente all'indirizzo IP da cui l'utente si è connesso all'inizio della sessione. In questo modo, nessuno può "rubare" la sessione dell'utente, poiché è richiesta la persistenza dell'IP. Questa configurazione è più sicura ma può causare problemi agli utenti che utilizzano un server proxy o una connessione Internet con assegnazione e modifica dinamiche degli indirizzi IP.

Usa la compressione HTTP
Selezionare questa casella di controllo per utilizzare la compressione HTTP nelle sessioni WorldClient.

Associa il server Web diWorldClient solo a queste porte o IP
Per limitare l'associazione del server WorldClient solo a a determinati indirizzi IP o porte, specificare gli indirizzi o le porte in questa casella separandoli con virgole. Utilizzare il formato: "Indirizzo_IP:Porta" per indicare la porta (ad esempio, 1.2.3.4:80). Se la porta non viene indicata, verranno utilizzate la porta TCP predefinita specificata in precedenza e la porta HTTPS predefinita specificata nella schermata SSL e HTTPS128. Se si desidera che WorldClient rimanga in ascolto su tutte le porte, utilizzare "*". Ad esempio, indicando "*,*:80" WorldClient rimane in attesa di connessioni da tutti gli indirizzi IP sulle porte predefinite specificate (3000 e 443), nonché di connessioni da tutti gli indirizzi IP sulla porta 80. Lasciando vuoto questo campo, WorldClient controlla tutti gli indirizzi IP specificati per il dominio predefinito41 e per i domini aggiuntivi115.

Riavvia WorldClient (necessario in caso di modifica della porta o del valore di IIS)
Fare clic su questo pulsante per riavviare il server WorldClient. Nota: dopo la modifica delle impostazioni della porta di WorldClient, è necessario riavviare WorldClient per rendere effettive le nuove impostazioni.

4.3.1.3.1.1 Esecuzione di WorldClient con IIS6

Poiché in WorldClient è incorporato un server Web, Internet Information Server (IIS) non è richiesto. WorldClient supporta comunque IIS e può pertanto funzionare come DLL ISAPI. Le informazioni seguenti, relative alla configurazione di WorldClient per il funzionamento con IIS6, sono riprese dall'articolo n. 01465 della MDaemon Knowledge Base, disponibile all'indirizzo www.altn.com:

1. Aprire la console di gestione di IIS (Internet Information Services).
2. Fare clic con il pulsante destro del mouse su **Pool applicazioni**.
3. Fare clic su **Nuovo/Pool applicazioni**.
4. Assegnare al pool il nome **Alt-N** e scegliere il pulsante **OK**.
5. Fare clic con il pulsante destro del mouse su **Alt-N**.
6. Fare clic su **Proprietà**.
7. Fare clic sulla scheda **Prestazioni**.
8. Deselezionare le opzioni **Chiudi processi di lavoro dopo un periodo di inattività di (in minuti)**: e **Limite massimo per la coda di richieste al kernel (numero di richieste).**
9. Fare clic sulla scheda **Identità**.
10. Nell'elenco a discesa Predefinito scegliere **Servizio locale**.
11. Fare clic sul pulsante **OK**.
12. Fare clic con il pulsante destro del mouse su **Siti Web**.
13. Scegliere **Nuovo**.
14. Fare clic su **Siti Web.** Verrà avviata una procedura guidata
15. Fare clic sul pulsante **Avanti**.
16. Digitare il nome del sito, ad esempio **WorldClient.**

17. Fare clic sul pulsante **Avanti.**
18. Fare nuovamente clic sul pulsante **Avanti.**
19. Selezionare la home directory, corrispondente a **C:\MDaemon\WorldClient\HTML** nel caso di un'installazione predefinita.
20. Fare clic sul pulsante **Avanti.**
21. Accertarsi che siano selezionate le opzioni **Lettura**, **Esecuzione script** ed **Esecuzione**.
22. Fare clic sul pulsante **Avanti**.
23. Fare clic sul pulsante **Fine**.
24. Fare clic con il pulsante destro del mouse sul sito Web appena creato **(WorldClient)**.
25. Scegliere **Proprietà**.
26. Fare clic sulla scheda **Documenti**.
27. Rimuovere tutti i documenti elencati.
28. Aggiungere **WorldClient.dll**.
29. Selezionare la scheda **Home directory.**
30. Nell'elenco a discesa Pool applicazioni, scegliere **Alt-N.**
31. Fare clic sul pulsante **OK.**
32. Fare clic su **Estensioni servizio Web.**
33. Abilitare **tutte le estensioni ISAPI sconosciute** o creare una nuova estensione relativa a **WorldClient.DLL**.

È necessario assegnare all'account Internet Guest, ossia a **IUSER_<SERVER_NAME>**, le autorizzazioni NTFS **Controllo completo** relative alla directory MDaemon e a tutte le relative sottodirectory.

1. Fare clic con il pulsante destro del mouse sulla directory MDaemon. (C:\MDaemon)
2. Scegliere **Proprietà**.
3. Selezionare la scheda **Sicurezza**.
4. Fare clic sul pulsante **Aggiungi**.
5. Fare clic sul pulsante **Avanzate**.
6. Fare clic sul pulsante **Trova**.
7. Selezionare **IUSER_<SERVER_NAME>** (in cui "<SERVER_NAME>" è il nome del computer locale).
8. Fare clic sul pulsante **OK.**
9. Fare clic sul pulsante **OK.**
10. Selezionare la casella **Controllo completo**.
11. Fare clic sul pulsante **OK.**

È necessario seguire questa procedura per tutte le directory da utilizzare con MDaemon.

Durante gli aggiornamenti di MDaemon successivi all'impostazione Web:

1. Aprire la console di gestione di IIS (Internet Information Services).
2. Aprire l'elenco **Pool applicazioni**.
3. Fare clic con il pulsante destro del mouse su **Alt-N.**
4. Scegliere **Arresta**.
5. Chiudere MDaemon.
6. Installare l'aggiornamento.
7. Al termine dell'installazione, riavviare MDaemon.
8. Nella console di gestione di IIS, fare clic con il pulsante destro del mouse su **Alt-N.**
9. Scegliere **Avvia**.

Se la procedura precedente è stata seguita correttamente, avviene quanto riportato di seguito.

1. Dopo l'arresto di **Pool applicazioni**, viene visualizzato un messaggio che informa che il **servizio non è disponibile**.
2. La procedura descritta riduce al minimo l'eventualità di dover riavviare il computer dopo un aggiornamento di MDaemon.

L'impostazione di questo programma con IIS NON è supportata dall'assistenza tecnica e se si sceglie di eseguire WC con IIS, è necessario essere consapevoli di tutti i problemi di sicurezza e delle implicazioni dell'esecuzione delle applicazioni con IIS. Prima di installare WorldClient come estensione ISAPI è consigliabile installare tutte le correzioni e gli aggiornamenti di IIS.

Quando viene eseguito con IIS, WorldClient non può essere avviato e chiuso dall'interfaccia di MDaemon. A questo scopo, è necessario utilizzare gli strumenti forniti con IIS.

4.3.1.3.2 SSL / HTTPS

Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). Il protocollo SSL, sviluppato da Netscape Communications Corporation, è il metodo standard per la protezione delle comunicazioni Web server/client e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare WebAdmin per l'utilizzo di HTTPS si trovano nella schermata SSL/HTTPS, disponibile in Impostazioni » Web, Sincronizzazione e Servizi IM » WebAdmin (configurazione Web)". Per praticità, tali impostazioni sono presenti anche in "Sicurezza» Impostazioni sicurezza » SSL e TLS » WorldClient".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e certificati** 311

Questa schermata è valida per WorldClient solo quando si utilizza il server Web incorporato di MDaemon. Se si configura WebAdmin per l'esecuzione con altri server Web quali IIS, queste opzioni non sono disponibili. Il supporto per SSL/HTTPS dovrà essere configurato con gli strumenti offerti dal server Web utilizzato.

Tipi di connessioni accettate

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a WorldClient. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in WorldClient, ma non si desidera imporre agli utenti di WorldClient l'utilizzo di HTTPS. WorldClient rimane in attesa di connessioni sulla porta HTTPS indicata di seguito, ma risponde anche alle normali connessioni HTTP sulla porta di WorldClient definita nella scheda Server Web 123 della schermata WorldClient (posta Web).

Solo HTTPS
Scegliere questa opzione se si desidera richiedere l'utilizzo di HTTPS al momento della connessione a WorldClient. Se si attiva questa opzione, WorldClient risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da WorldClient per le connessioni SSL. La porta SSL predefinita è 443. Se si utilizza la porta predefinita, per le connessioni HTTPS non è necessario includere il numero della porta nell'URL di WorldClient (vale a dire, "https://esempio.com" è equivalente a "https://esempio.com:443").

Questa porta è diversa dalla porta di WorldClient definita nella scheda Server Web 123 della schermata WorldClient (posta Web). Se le connessioni HTTP a WorldClient sono consentite, devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

Certificati

Questa casella consente di visualizzare i certificati SSL. Per definire il certificato da utilizzare in WorldClient, selezionarlo dall'elenco. Fare doppio clic sul certificato per aprire la finestra di dialogo Certificato che consente di visualizzarne o modificarne i dettagli.

MDaemon non consente l'utilizzo di più certificati per WorldClient. Tutti i domini WorldClient devono condividere un unico certificato. Qualora sia disponibile più di un dominio, inserire i nomi di tali domini e di quelli che si intende utilizzare per accedere a WebAdmin nel campo denominato "*Nomi host alternativi (separare le voci con una virgola)*" descritto di seguito.

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wc.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Il supporto di più certificati non è disponibile. Tutti i domini WorldClient devono condividere un unico certificato. Qualora per le connessioni degli utenti esistano nomi host alternativi, inserire i nomi dei domini separati da virgole nel caso in cui si intenda applicare il certificato anche ai nomi alternativi. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Crea certificato
Dopo aver inserito tutte le informazioni nei controlli descritti in precedenza, per creare il certificato fare clic su questo pulsante.

Riavvia server Web
Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare i nuovi certificati, è necessario riavviare il server Web.

Per ulteriori informazioni, vedere:

SSL e certificati 311
Creazione e uso dei certificati SSL 320

4.3.1.3.3 ComAgent/IM

Questa finestra di dialogo determina diversi aspetti dell'applet ComAgent visualizzata nella barra delle applicazioni e della messaggistica istantanea. È possibile impostare queste opzioni per i singoli domini.

ComAgent/IM

Seleziona dominio
Utilizzare questo elenco a discesa per scegliere il dominio di cui si desidera modificare le impostazioni. Utilizzare il dominio *Default* per modificare le impostazioni predefinite. Le impostazioni predefinite vengono utilizzate per tutti i domini le cui impostazioni non sono state specificamente modificate. Se si apportano delle modifiche alle impostazioni e si tenta di selezionare un dominio diverso da quelli presenti nell'elenco, verrà chiesto di specificare se salvare le modifiche prima di passare al nuovo dominio. Fare clic su *Sì* per salvare le modifiche o su *No* per annullare l'operazione.

Abilita supporto per ComAgent
Selezionare questa opzione per rendere disponibile l'utilità di messaggistica istantanea ComAgent agli utenti del dominio selezionato. L'utilità può essere scaricata dalla pagina Opzioni » ComAgent di WorldClient. Il file di installazione scaricato viene personalizzato automaticamente in base all'account di ciascun utente, così da facilitare l'installazione e la configurazione.

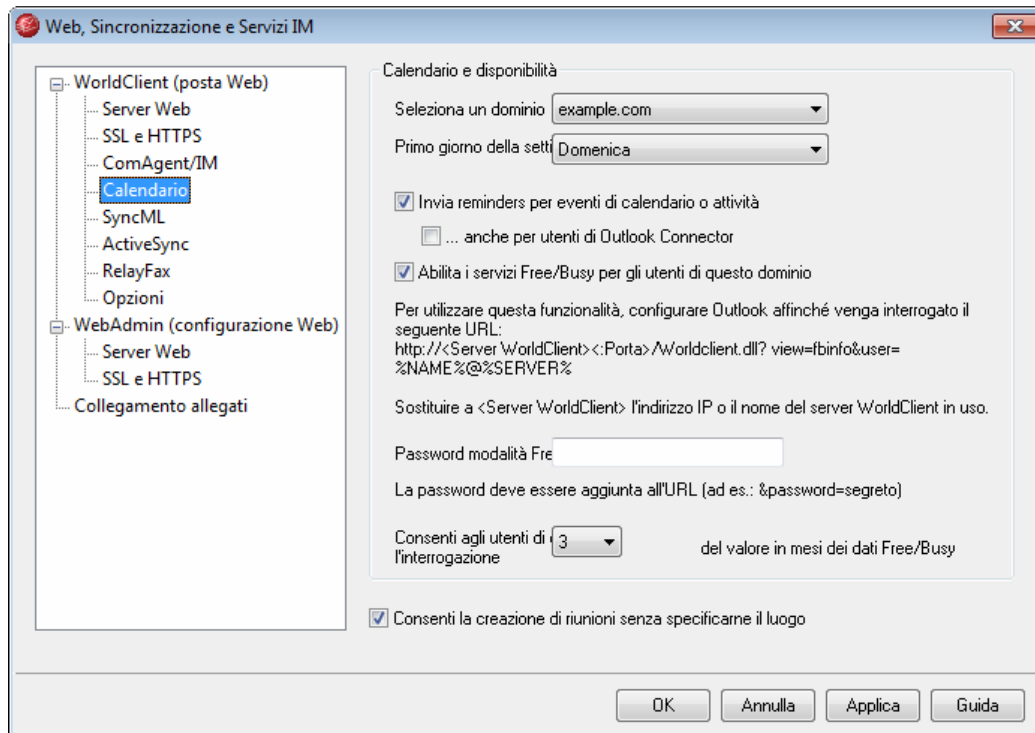
Abilita messaggistica istantanea
Selezionare questa opzione per attivare il sistema di messaggistica istantanea (IM) di ComAgent per gli utenti del dominio selezionato. Deselezionare la casella di

controllo per impedire l'uso dei comandi di messaggistica istantanea.

Registra tutto il traffico IM a livello server
Selezionare questa casella di controllo se si desidera che tutto il traffico relativo ai messaggi istantanei del dominio selezionato venga incluso nel file `InstantMessaging.log`, situato nella cartella `MDaemon/LOGS/`.

L'elenco dei compagni di conversazione IM include i membri di altri domini
Selezionare questa opzione se si desidera che agli elenchi dei compagni di conversazione del dominio selezionato possano essere aggiunti gli utenti di MDaemon, indipendentemente dal dominio. Deselezionare questa casella di controllo per fare in modo che agli elenchi dei compagni di conversazione possano essere aggiunti solo gli utenti dello stesso dominio. Se ad esempio MDaemon effettua l'hosting di esempio.com e nomeazienda.com, attivando questo comando per esempio.com, agli utenti di tale dominio viene consentito di aggiungere i compagni di conversazione agli elenchi di entrambi i domini. Deselezionando l'opzione, gli utenti possono aggiungere solo altri utenti di esempio.com.

I promemoria inviati mediante il sistema IM vengono inviati dall'indirizzo indicato come 'From:' [*testo*]
Quando sul calendario di un utente di WorldClient è pianificato un appuntamento, è possibile impostare l'evento in modo che all'utente venga inviato un promemoria a un'ora specifica. Quando per il dominio dell'utente il sistema IM è attivo, il promemoria viene inviato in un messaggio istantaneo, se l'utente sta utilizzando ComAgent. Utilizzare questa casella di testo per specificare che si desidera che il messaggio compaia come proveniente dall'indirizzo indicato nel campo 'From:'.

4.3.1.3.4 Calendario

Calendario e disponibilità

Seleziona un dominio
Utilizzare questo elenco a discesa per scegliere il dominio di cui si desidera modificare le impostazioni di pianificazione di gruppo e calendario. Se si apportano delle modifiche alle impostazioni e si tenta di selezionare un dominio diverso, verrà chiesto di specificare se salvare le modifiche prima di passare al nuovo dominio. Fare clic su *Sì* per salvare le modifiche o su *No* per annullare l'operazione.

Primo giorno della settimana
Scegliere un giorno dall'elenco a discesa. La selezione verrà visualizzata nei calendari del dominio come primo giorno della settimana.

Invia reminder per eventi di calendario o attività
Selezionare questa casella di controllo per consentire l'invio agli utenti del calendario e dei promemoria delle attività di WorldClient tramite posta elettronica e ComAgent.

...anche a utenti Outlook Connector
Se l'opzione "*Invia reminder per eventi di calendario o attività*" è attivata, selezionare questa opzione se si desidera attivare i promemoria anche per gli utenti Outlook Connector.

Opzioni modalità Free/Busy

MDaemon include un server Free/Busy che consente a un pianificatore di riunioni di visualizzare la disponibilità dei potenziali partecipanti. Per accedere a questa

funzione, fare clic su Pianificazione in WorldClient quando si crea un nuovo appuntamento. Viene aperta la finestra Pianificazione che contiene l'elenco dei partecipanti e una griglia calendario con codifica cromatica che presenta una riga per ciascuno dei partecipanti. La riga relativa a ciascun partecipante ha un codice di colore che indica l'ora in cui è disponibile per una riunione. Ai colori corrispondono le modalità Occupato, Incerto, Fuori sede e Nessuna informazione. Con il pulsante Passa al successivo è inoltre possibile interrogare il server a proposito della successiva fascia oraria in cui tutti i partecipanti potrebbero essere disponibili. Al termine della creazione dell'appuntamento, verrà inviato un invito a tutti i partecipanti che potranno quindi accettarlo o declinarlo.

Il server Free/Busy di WorldClient è inoltre compatibile con Microsoft Outlook. Per utilizzarlo, configurare Outlook affinché venga interrogato il seguente URL per cercare dati relativi alla disponibilità. Ad esempio, in Outlook 2002 le opzioni Free/Busy si trovano in "Strumenti » Opzioni » Opzioni calendario » Opzioni disponibilità".

URL del server Free/Busy per Outlook:

```
http://<WorldClient><:Porta>
/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER%
```

Sostituire "`<WorldClient>`" con l'indirizzo Ip o il nome dominio del server WorldClient e "`<:Porta>`" con il relativo numero di porta se non si utilizza la porta Web predefinita. Ad esempio,

```
http://esempio.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%
SERVER%
```

Per ulteriori informazioni sull'utilizzo delle funzioni di Free/Busy di WorldClient per la pianificazione degli appuntamenti, vedere la Guida in linea di WorldClient.

Abilita i servizi Free/Busy per gli utenti di questo dominio
Fare clic su questa opzione se si desidera consentire l'accesso alle funzioni del server Free/Busy agli utenti del dominio selezionato in precedenza.

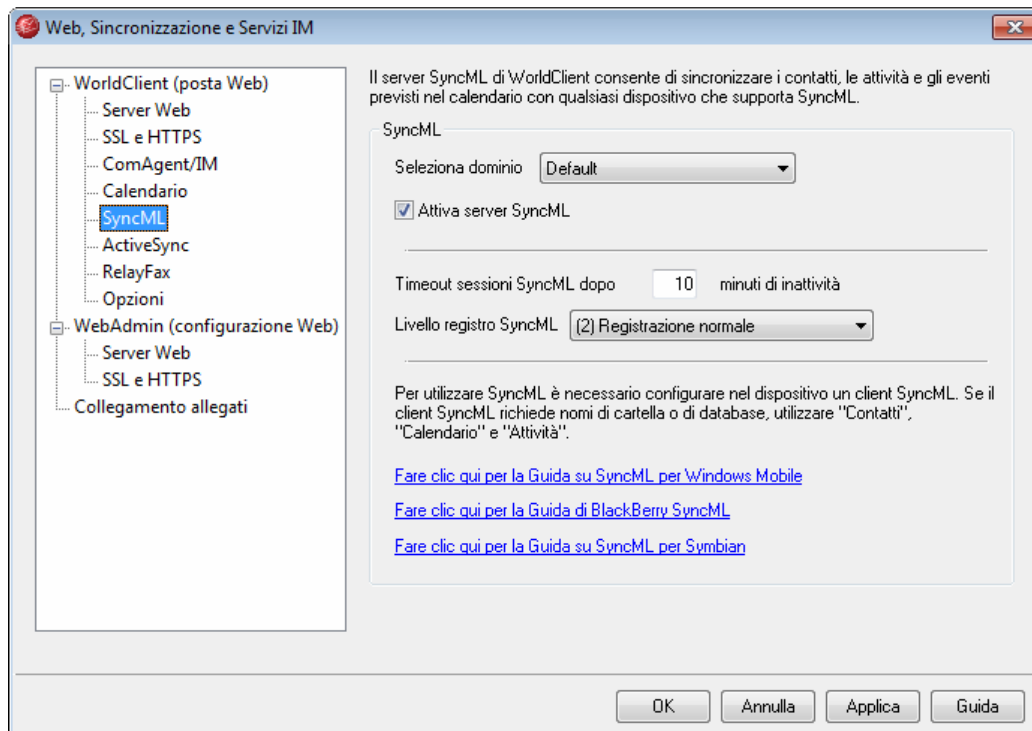
Password modalità Free/Busy
Se si desidera richiedere una password agli utenti del dominio che tentano di accedere alle funzioni del server Free/Busy tramite Outlook, inserire in questo campo la password. È necessario aggiungere la password all'URL (nel formato: "`&password=FBServerPass`") quando vengono configurate le impostazioni di disponibilità in Outlook. Ad esempio,

```
http://esempio.com:3000/Worldclient.dll?view=fbinfo&user=%NAME%@%SERVER
%&password=MyFBServerPassword
```

Consenti agli utenti di eseguire l'interrogazione del valore in mesi dei dati Free/Busy
Utilizzare questa opzione per specificare l'intervallo dei dati relativi alla disponibilità che è possibile interrogare, espresso in numero di mesi.

Opzioni per le riunioni

Consenti la creazione di riunioni senza specificarne il luogo
Selezionare questa opzione se non si desidera che gli utenti debbano specificare il luogo della riunione quando viene creato un evento riunione. Deselezionare questa casella di controllo se si desidera imporre che per tutte le riunioni venga specificato un luogo al momento della pianificazione. Si tratta di un'impostazione globale che non può essere specificata a livello di singolo dominio.

4.3.1.3.5 SyncML

WorldClient comprende un server SyncML che consente di sincronizzare i contatti, le attività e gli eventi di calendario con quelli di qualsiasi dispositivo mobile compatibile con SyncML. Se lo smartphone BlackBerry o altri dispositivi non prevedono il supporto incorporato SyncML, è necessario installare un client di sincronizzazione di terze parti. Alcuni esempi di client sono: Funambol Sync Client, Synthesis e SyncJE. Esistono anche client in grado di sincronizzare il calendario con un client di posta elettronica come Microsoft Outlook. Il client Funambol Sync, ad esempio, è disponibile per Outlook, BlackBerry, Windows Mobile e per altri tipi di applicazioni e di dispositivi. Numerosi client sono gratuiti.

Per ulteriori informazioni su SyncML e sulla specifica SyncML, visitare il sito OMA (Open Mobile Alliance) all'indirizzo:.

SyncML

Seleziona dominio
La casella di riepilogo a discesa consente di selezionare il dominio da configurare. Dopo aver selezionato il dominio, selezionare o deselezionare la casella "*Attiva server SyncML*" e fare clic su Applica o su OK per salvare l'impostazione. Scegliere "Predefinito" dall'elenco a discesa per assegnare l'impostazione predefinita. Le impostazioni predefinite verranno applicate a tutti i nuovi domini e a tutti i domini esistenti per cui non è stata definita un'impostazione SyncML specifica.

Attiva server SyncML
Selezionare o deselezionare questa opzione per specificare l'accessibilità del server SyncML dal dominio selezionato nell'opzione *Seleziona dominio* descritta in precedenza.

Timeout sessioni SyncML dopo XX minuti di inattività
Rappresenta la durata di tempo per cui è consentita l'inattività di una sessione SyncML prima che essa scada e venga chiusa automaticamente. Si tratta di un'impostazione globale che viene applicata a tutte le sessioni SyncML, indipendentemente dal dominio.

Livello registro SyncML
Questo elenco a discesa consente di specificare il livello di dettaglio utilizzato per registrare le attività SyncML. Sono disponibili sei possibili livelli di registrazione: 1 - registrazione debug; 2 - registrazione normale; 3 - solo avvisi e errori; 4 - solo errori; 5 - solo errori critici; 6 - nessuna registrazione. Si tratta di un'impostazione globale che non può essere applicata a specifici domini.

4.3.1.3.5.1 Configurazione dei client SyncML

Per accedere al server SyncML di WorldClient, è necessario configurare i client SyncML per la connessione a:

```
http://<Server WorldClient><:porta>/MDSyncML.dll
```

Esempi:

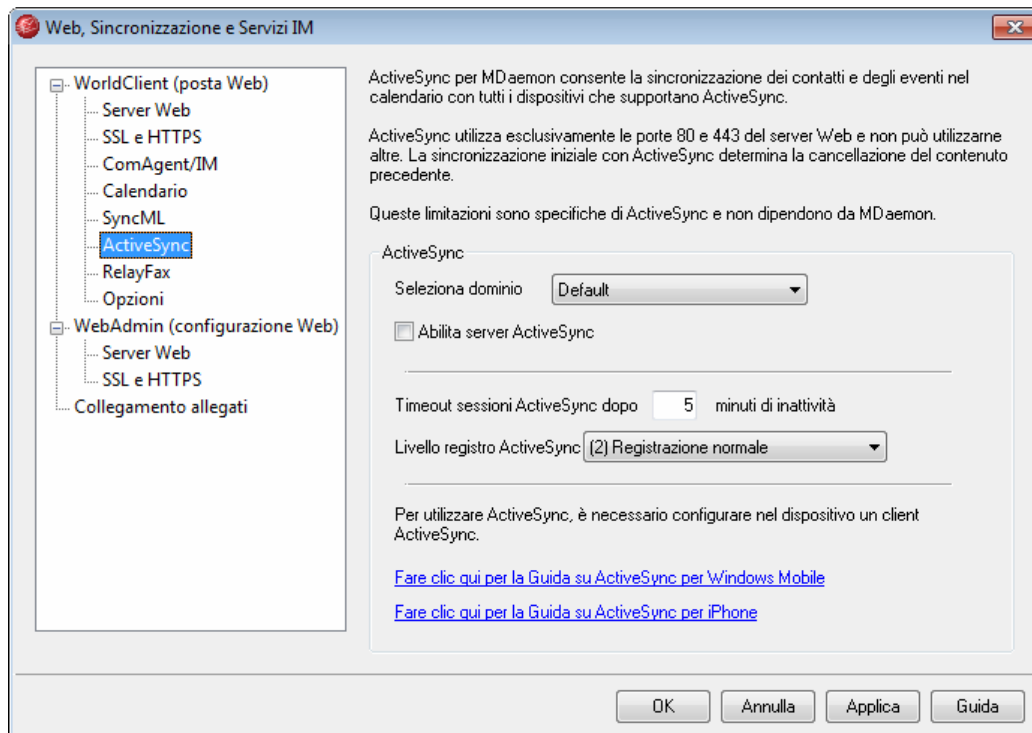
```
http://mail.esempio.com:3000/MDSyncML.dll
http://www.esempio.com/MDSyncML.dll
```

Se il client SyncML richiede i nomi delle cartelle, utilizzare `Contatti`, `Calendario` e `Attività`. Tali nomi vengono sempre sostituiti con le corrispondenti cartelle WorldClient predefinite dell'utente.

Per indicare i percorsi per le cartelle, il server SyncML supporta i seguenti formati:

`contatti`
`/contatti`
`./contatti`
`contatti/telefono` (supponendo che esista una sottocartella telefono)
`contatti.imap\telefono.imap`

Prima di eseguire la sincronizzazione con SyncML, è necessario effettuare l'accesso a WorldClient almeno una volta.

4.3.1.3.6 ActiveSync

MDaemon supporta anche "ActiveSync per MDaemon," un server ActiveSync (AirSync) con una licenza OTA concessa separatamente. Questo server è in grado di sincronizzare il calendario e i contatti predefiniti dell'utente tra l'account MDaemon/ WorldClient e un dispositivo ActiveSync. Le opzioni ActiveSync di MDaemon si trovano in: Impostazioni » Web, Sincronizzazione e Servizi IM... » ActiveSync e un'opzione nella schermata Opzioni374 di Account Editor consente di disattivarle per alcuni utenti.

Alla prima attivazione per MDaemon, ActiveSync offre 30 giorni in modalità di prova. In seguito, per continuare a utilizzarlo, è necessario acquistare la licenza pagandone il costo un'unica volta. È possibile acquistare la chiave di licenza presso www.altn.com o presso il proprio rivenditore/distributore locale.

ActiveSync è l'estensione di un servizio Web che opera solo con le porte **80** (per http) e **443** (per https). Non è possibile utilizzare ActiveSync su altre porte. **ActiveSync non funziona se il server Web**123 **integrato di WorldClient o l'eventuale altro server in uso, ad esempio IIS, non utilizza la porta 80 e/o 443.** Questo è un requisito di implementazione di ActiveSync.

È possibile utilizzare l'opzione "**Associa il server Web di WorldClient solo a queste porte o IP**" della schermata WorldClient (posta Web) » Server Web 123 per fare in modo che MDaemon rimanga in attesa di connessioni sia dalla porta 80 che da quella predefinita, indicata nella stessa schermata.

Per eseguire ActiveSync con IIS è necessario chiamare la libreria DLL ActiveSync (`MDAirSync.dll`) quando viene richiesto "`/Microsoft-Server-ActiveSync`". Questa richiesta è utilizzata da tutti i client ActiveSync. Alcune versioni di IIS non consentono questa funzione senza aver preventivamente scaricato, installato e configurato un software di terze parti.

Tutte le sincronizzazioni iniziali con ActiveSync sono unilaterali dal server al dispositivo. I dati del dispositivo vengono persi durante la prima sincronizzazione con ActiveSync. Questo è un requisito di implementazione di ActiveSync. Pertanto si consiglia di effettuare il backup dei dati del dispositivo prima di utilizzare ActiveSync per la prima volta. La maggior parte dei dispositivi dotati del supporto ActiveSync avvisa l'utente che "**tutti i dati del dispositivo andranno persi**," ma non tutti. Gestire la funzionalità ActiveSync con attenzione.

Attivazione/disattivazione di ActiveSync

Per attivare o disattivare ActiveSync, selezionare un dominio nell'elenco a discesa e selezionare o deselezionare **Abilita server ActiveSync**.

Impostazione del valore di timeout della sessione ActiveSync

L'opzione *Timeout sessioni ActiveSync dopo [xx] minuti di inattività* consente di specificare la durata dell'inattività di una sessione ActiveSync prima del timeout.

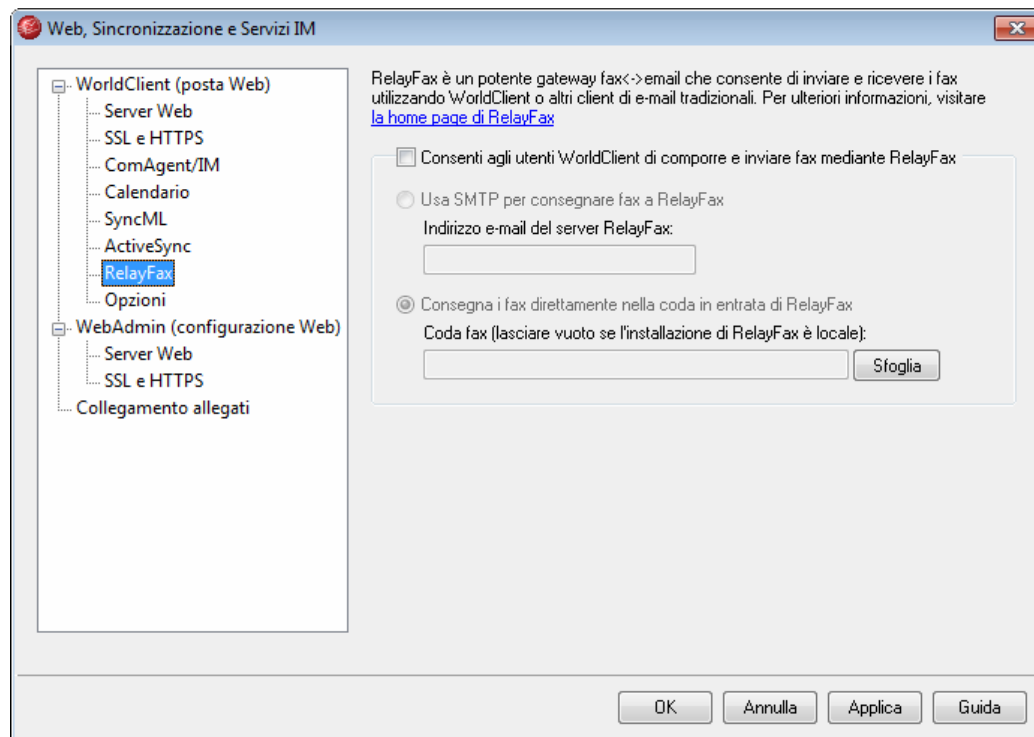
Livello di registrazione di ActiveSync

ActiveSync per MDaemon prevede sei livelli di registrazione, da *(1) registrazione debug* a *(6) nessuna registrazione*. *(1) registrazione debug* viene generalmente utilizzato per la diagnosi dei problemi. L'impostazione *(2) registrazione normale* offre una quantità di dati adeguata e rappresenta l'impostazione predefinita.

Per utilizzare ActiveSync è necessario configurare nel dispositivo dell'utente un client ActiveSync. Per istruzioni, fare clic sui collegamenti della finestra di dialogo ActiveSync di MDaemon.

Vedere:

[Account Editor » Opzioni] 374
[Server Web] 123

4.3.1.3.7 RelayFax

Il server RelayFax di Alt-N Technologies è un gateway e-mail verso fax o fax verso e-mail, che può essere efficacemente integrato con WorldClient per offrire servizi agli utenti. Quando questa funzionalità è abilitata, gli utenti di WorldClient possono accedere a una serie di risorse per la composizione e l'invio di fax dalle schermate del client WorldClient. Per ulteriori informazioni, visitare la sezione RelayFax di www.altn.com.

Opzioni di integrazione di RelayFax

Consenti all'utente WorldClient di creare e inviare fax con RelayFax
Selezionare questa opzione per integrare RelayFax con WorldClient. Una volta attivato il server RelayFax, nelle pagine di WorldClient vengono visualizzati il comando Componi fax e altre funzioni correlate.

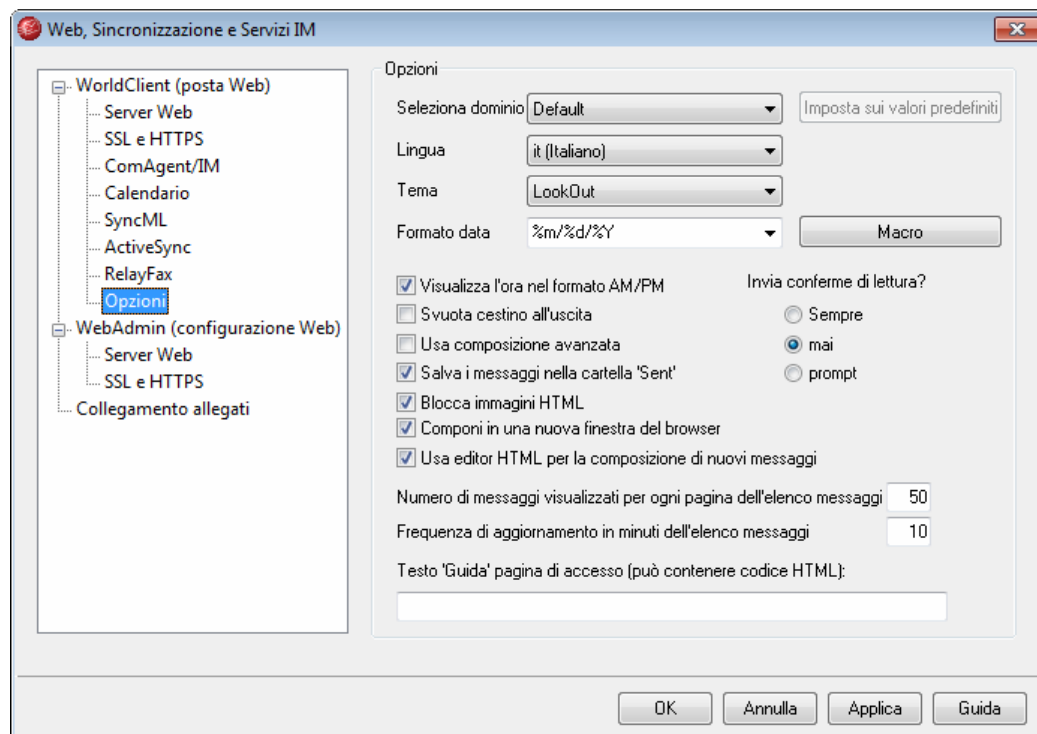
Usa SMTP per consegnare fax a RelayFax
Il server RelayFax controlla una specifica casella postale per verificare la presenza di messaggi in entrata da trasmettere via fax. Selezionare questa opzione affinché MDaemon invii tali messaggi all'indirizzo della casella postale in questione mediante il normale processo di trasmissione SMTP. Questa opzione è utile quando il server

RelayFax controlla una casella postale non situata nella rete LAN in uso. Se il server RelayFax è installato nella rete in uso, è possibile impostare MDaemon affinché trasmetta i messaggi direttamente alla coda di posta del server RelayFax, saltando l'intero processo di trasmissione SMTP. Per ulteriori informazioni, vedere *Consegna i fax direttamente nella coda in entrata di RelayFax* più avanti in questo capitolo.

Indirizzo e-mail del server RelayFax
In questo campo viene specificato l'indirizzo e-mail a cui consegnare i messaggi trasmessi via fax. Il valore deve corrispondere all'indirizzo specificato in RelayFax per il monitoraggio di questo tipo di messaggi.

Consegna i fax direttamente nella coda in entrata di RelayFax
Se il server RelayFax è residente sulla LAN in uso, per la distribuzione dei messaggi da inviare via fax è possibile scegliere questo metodo anziché la trasmissione SMTP. Quando il server MDaemon riceve un messaggio destinato a RelayFax, lo consegna direttamente nella coda in entrata di RelayFax, anziché trasmetterlo via SMTP.

Coda fax
Se il server RelayFax è installato nello stesso sistema su cui è in esecuzione il server MDaemon, il campo del percorso del file può essere lasciato vuoto; in caso contrario, è necessario specificare il percorso di rete della directory \app\ del server RelayFax.

4.3.1.3.8 Opzioni

Le impostazioni di questa schermata sono specifiche per il dominio e controllano il

comportamento a livello di client, anziché il comportamento e la configurazione a livello globale del server WorldClient.

Opzioni

Seleziona dominio
Utilizzare questo elenco a discesa per scegliere il dominio di cui si desidera modificare le impostazioni. Utilizzare il dominio *Default* per modificare le impostazioni predefinite. Le impostazioni predefinite vengono utilizzate per tutti i domini le cui impostazioni non siano state specificamente modificate. Se si apportano delle modifiche alle impostazioni e si tenta di selezionare un dominio diverso da quelli presenti nell'elenco, verrà chiesto di specificare se salvare le modifiche prima di passare al nuovo dominio. Fare clic su *Sì* per salvare le modifiche o su *No* per annullare l'operazione.

Imposta sui valori predefiniti
Questa impostazione consente di reimpostare le impostazioni *predefinite* del dominio. Selezionare un dominio mediante il comando *Seleziona dominio*, quindi fare clic su *Imposta sui valori predefiniti* per ripristinarne le impostazioni originarie.

Lingua

Utilizzare questa casella di riepilogo a discesa per scegliere la lingua predefinita con cui l'interfaccia di WorldClient viene visualizzata agli utenti durante la prima registrazione al dominio selezionato. Gli utenti possono modificare le impostazioni personali della lingua mediante la pagina Entra e mediante un'opzione di Opzioni » Personalizza di WorldClient.

Tema

Questa casella di riepilogo a discesa consente di indicare il tema predefinito di WorldClient da utilizzare per il primo accesso degli utenti al dominio selezionato. È possibile personalizzare l'impostazione del tema mediante Opzioni » Personalizza di WorldClient.

Formato data
Utilizzare questa casella di testo per specificare la formattazione delle date per il dominio selezionato. Fare clic su Il pulsante Macro consente di visualizzare un elenco di codici macro utilizzabili nella casella di testo. Sono disponibili le seguenti macro:

%A - Nome completo del giorno

%B - Nome completo del mese

%d - Giorno del mese (visualizzato nel formato "01-31")

%m - Mese (visualizzato nel formato "01-12")

%y - Anno nel formato a 2 cifre

%Y - Anno nel formato a 4 cifre

Ad esempio, la data "`%d/%m/%Y`" viene visualizzata in WorldClient nel modo seguente "`25/12/2002`".

Questa impostazione è specifica per il dominio. I singoli utenti non possono modificare il formato data utilizzato per i propri account.

Macro
Fare clic su questo pulsante per visualizzare un elenco di codici macro utilizzabili in *Formato data*.

Visualizza l'ora nel formato AM/PM
Selezionare questa opzione se si desidera che in WorldClient l'ora del dominio selezionato venga visualizzata nel formato orario a 12 ore (AM/PM). Deselezionare questa casella di controllo per utilizzare il formato a 24 ore. I singoli utenti possono modificare questa impostazione mediante l'opzione "*Visualizza gli orari in formato AM/PM*" situata nella pagina Opzioni » Calendario di WorldClient.

Svuota cestino all'uscita
Selezionando questa opzione, il cestino dell'utente verrà svuotato all'uscita da WorldClient. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Personalizza di WorldClient.

Usa composizione avanzata
Abilitare questa casella se si desidera che, per impostazione predefinita, gli utenti del dominio visualizzino la schermata Composizione avanzata di WorldClient, anziché la normale schermata Componi. I singoli utenti possono modificare questa impostazione in Opzioni » Componi di WorldClient.

Salva i messaggi nella cartella 'Sent'
Selezionare questa opzione se si desidera che una copia di ogni messaggio inviato venga salvata nella cartella *Sent* (Posta inviata) della casella postale. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Componi di WorldClient.

Blocca immagini HTML
Questa casella di controllo consente di impedire la visualizzazione automatica di immagini remote durante la visualizzazione di messaggi di posta elettronica HTML con WorldClient. Per visualizzare le immagini, è necessario selezionare la barra visualizzata al di sopra del messaggio nella finestra del browser. Si tratta di una funzione anti spam, perché molti messaggi spam contengono immagini con particolari URL che identificano l'indirizzo di posta elettronica dell'utente che ha visualizzato le immagini, confermando così al mittente che si tratta di un indirizzo valido e operativo. L'opzione è abilitata per impostazione predefinita.

Componi in una nuova finestra del browser
Selezionare questa casella se si desidera che per la composizione dei messaggi venga aperta una nuova finestra del browser. In caso contrario, si passerà dalla finestra principale alla schermata di composizione. Deselezionare la casella se non si desidera che venga aperta una finestra separata. I singoli utenti possono modificare questa impostazione nella pagina Opzioni » Componi di WorldClient.

Usa editor HTML per la composizione di nuovi messaggi
Abilitare questa casella se si desidera che, per impostazione predefinita, gli utenti del dominio possano visualizzare l'editor di composizione HTML di WorldClient. I singoli utenti possono modificare questa impostazione in Opzioni » Componi di WorldClient.

Invia conferme di lettura
Questa opzione determina la risposta di WorldClient ai messaggi in arrivo che contengono una richiesta di conferma di lettura.

sempre
Selezionando questa opzione, MDaemon invia una notifica di avvenuta lettura al mittente. All'utente di WorldClient che ha ricevuto il messaggio non viene segnalato che è stata richiesta o soddisfatta una conferma di lettura.

mai
Questa opzione indica a WorldClient di ignorare le richiesta di conferma di lettura.

prompt
Con questa opzione, agli utenti di WorldClient viene richiesto se inviare una conferma di lettura ogni volta che viene aperto un messaggio che lo richiede.

Numero di messaggi visualizzati per ogni pagina dell'elenco messaggi
Indica il numero di messaggi che vengono visualizzati su ciascuna pagina dell'elenco dei messaggi per ogni cartella di posta. Se in una cartella è contenuto un numero di messaggi superiore a quello specificato in questo campo, sopra e sotto l'elenco verranno visualizzati dei comandi che consentono di passare alle altre pagine. I singoli utenti possono modificare questa impostazione in Opzioni » Personalizza di WorldClient.

Frequenza di aggiornamento in minuti dell'elenco messaggi
Indica per quanti minuti WorldClient attende prima di aggiornare automaticamente l'elenco dei messaggi. I singoli utenti possono modificare questa impostazione in Opzioni » Personalizza di WorldClient.

Testo 'Guida' pagina di accesso (può contenere codice HTML)
Questa opzione consente di specificare una frase testuale, in testo semplice o HTML, da visualizzare nella schermata di registrazione di WorldClient quando si verifica un problema di accesso. Il testo viene visualizzato al di sotto del seguente testo predefinito: "*Accesso errato, riprovare. Se è necessaria assistenza, contattare l'amministratore della posta elettronica.*" Il testo può essere utilizzato per dirigere gli utenti a una data pagina o per ottenere informazioni relative all'accesso a WorldClient.

4.3.2 WebAdmin (configurazione Web)

WebAdmin è un'applicazione progettata appositamente per fornire il supporto alla gestione remota basata su Web del software di Alt-N Technologies. Viene fornita con MDaemon e supporta l'amministrazione remota sia di MDaemon® che del relativo componente e-mail integrato basato su Web, WorldClient®.

WebAdmin è un'applicazione server progettata per essere eseguita in background sullo stesso computer nel quale è in esecuzione MDaemon. Per accedere a WebAdmin, è sufficiente aprire il browser e digitare l'URL e il numero di porta relativi a WebAdmin, ad esempio `www.mywebadmin.com:1000`. Una volta fornite le credenziali appropriate, l'utente avrà accesso ai controlli e alle impostazioni di MDaemon. Il tipo e il numero delle impostazioni che possono essere gestite dipendono dal livello di accesso fornito, ovvero Globale, Dominio o Utente.

Amministratori globali - Si tratta di utenti per cui sono abilitate autorizzazioni di accesso globale nelle relative impostazioni di account in MDaemon. Se usufruisce di accesso globale, l'utente può visualizzare e configurare tutte le impostazioni e tutti i controlli accessibili via WebAdmin. Gli amministratori globali possono aggiungere, modificare ed eliminare utenti, domini e liste di distribuzione. Grazie al completo controllo amministrativo, sono inoltre in grado di modificare i file INI dei prodotti, specificare altri utenti come amministratori di dominio, gestire le password e altro.

Amministratori di dominio - Analogamente agli amministratori globali, quelli di dominio hanno il controllo completo su tutti gli utenti e le impostazioni di prodotto accessibili via Web. Tuttavia, tale controllo è limitato ai domini a cui hanno accesso. Gli amministratori di dominio e i domini sui quali esercitano il controllo vengono specificati all'interno di WebAdmin da un amministratore globale o da un altro amministratore di dominio che ha accesso ai domini in questione.

Utenti - Il livello minimo previsto per l'accesso a WebAdmin è l'accesso utente. Gli utenti MDaemon, ad esempio, possono accedere a WebAdmin e visualizzare le proprie impostazioni di account, nonché modificare le voci MultiPOP, i filtri

applicati alla posta, le risposte automatiche e così via. Il tipo e il numero delle impostazioni modificabili si basano sulle autorizzazioni fornite nelle impostazioni di account di ciascun utente.

Qualsiasi utente che abbia l'autorizzazione ad accedere sia a WorldClient che a WebAdmin può accedere a quest'ultimo da WorldClient. È possibile aprire WebAdmin in una finestra separata del browser da WorldClient facendo clic sul collegamento "Impostazioni avanzate" in "Opzioni".

Per ulteriori informazioni, vedere:

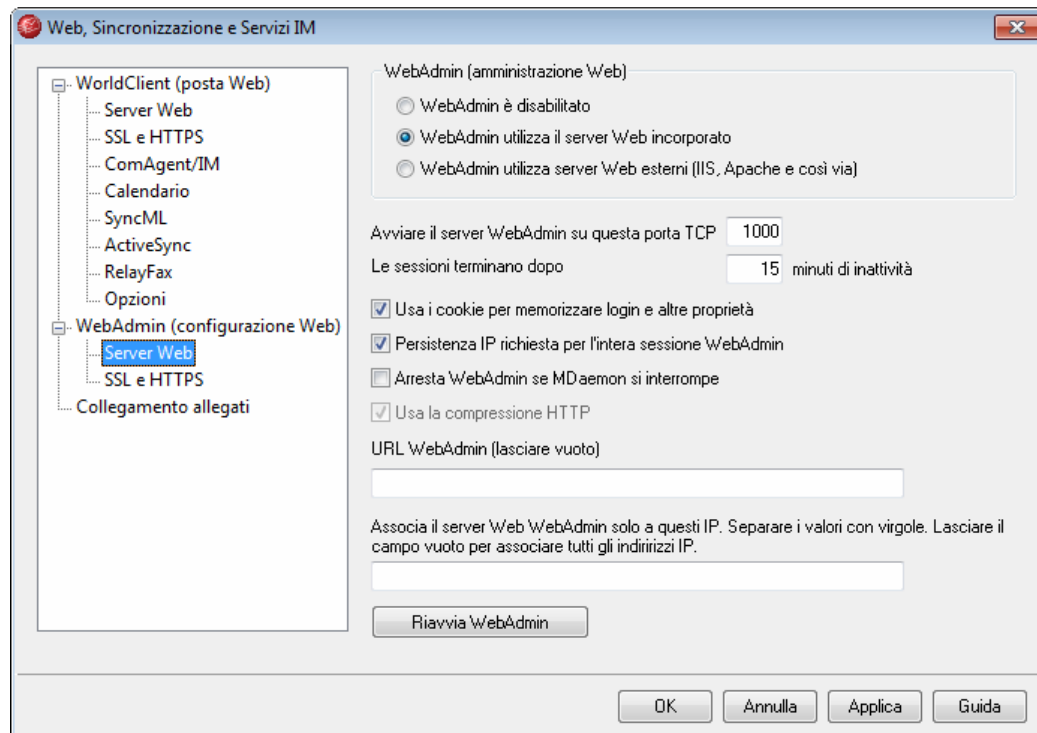
WebAdmin » Server Web 145

WebAdmin » HTTPS 147

Valori predefiniti nuovo account » Accesso Web 382

Account Editor » Accesso Web 347

Esecuzione di WebAdmin con IIS 150

4.3.2.1 Server Web

WebAdmin (amministrazione Web)

WebAdmin è disabilitato
Scegliere questa opzione per disabilitare WebAdmin. Il server WebAdmin può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon.

WebAdmin utilizza il server Web incorporato
Scegliere questa opzione per eseguire WebAdmin utilizzando il server Web incorporato di MDaemon. Il server WebAdmin può essere abilitato/disabilitato anche dal menu File o dalla sezione Server del riquadro Statistiche dell'interfaccia principale di MDaemon

WebAdmin utilizza server Web esterni (IIS, Apache e così via)
Scegliere questa opzione se si desidera eseguire WebAdmin in Internet Information Server (IIS) o in un altro server Web diverso dal server incorporato di MDaemon. In questo modo, è possibile impedire l'accesso a elementi della GUI che potrebbero entrare in conflitto con il server alternativo.

Per ulteriori informazioni, vedere Esecuzione di WebAdmin con IIS 150.

Avviare il server WebAdmin su questa porta TCP
Si tratta della porta da cui WebAdmin rileverà le connessioni provenienti dal browser Web. La porta predefinita è 1000.

Le sessioni terminano dopo XX minuti di inattività
Una volta ottenuto l'accesso a WebAdmin, le sessioni possono rimanere inattive per il tempo specificato in questo campo prima di venire chiuse. Il valore predefinito è di 15 minuti.

Usa i cookie per memorizzare login e altre proprietà
Selezionare questa opzione se si desidera che WebAdmin archivi l'ID utente e altre specifiche proprietà in un cookie sul computer locale. Questa funzione consente di offrire agli utenti un accesso più "personalizzato", purché nel browser sia abilitato il supporto per i cookie.

Persistenza IP richiesta per l'intera sessione WebAdmin
Come misura di sicurezza aggiuntiva, è possibile selezionare questa casella di controllo in modo che WebAdmin limiti ciascuna sessione utente all'indirizzo IP da cui si è connesso l'utente all'inizio della sessione. Poiché è richiesta la persistenza dell'IP, nessuno potrà "appropriarsi" della sessione dell'utente. Questa configurazione è più sicura ma può generare problemi quando si utilizza un server proxy o una connessione Internet che assegna e modifica dinamicamente gli indirizzi IP.

Arresta WebAdmin se MDaemon si interrompe
Fare clic su questa opzione se si desidera chiudere WebAdmin quando viene chiuso MDaemon. In caso contrario, WebAdmin continua ad essere eseguito in background.

URL WebAdmin
Rappresenta l'URL utilizzato da WorldClient internamente quando si fa clic sul collegamento Impostazioni avanzate per modificare le impostazione degli account tramite WebAdmin. Lasciare vuoto questo campo se WebAdmin viene eseguito con il server Web incorporato. Se si utilizza un server Web alternativo come l'IIS e WebAdmin è stato configurato per essere eseguito in un URL o in un indirizzo IP alternativi, specificare l'URL in questo campo.

Associa il server Web di WebAdmin solo a questi IP
Per limitare l'associazione del server WebAdmin solo a determinati indirizzi IP, specificare tali indirizzi in questa casella separandoli con virgole. Lasciando vuoto questo campo, il server WorldClient controlla tutti gli indirizzi IP specificati per il dominio predefinito[41] e per i domini aggiuntivi[115].

Riavvia WebAdmin (se cambiano porte o parametri di IIS)
Fare clic su questo pulsante per riavviare il server WebAdmin. Nota: quando si modificano le impostazioni della porta, è necessario riavviare WebAdmin per rendere effettive le nuove impostazioni.

Vedere:

WebAdmin (configurazione Web)[144]
WebAdmin » HTTPS[147]
Esecuzione di WebAdmin con IIS[150]
Valori predefiniti del nuovo account » WorldClient e WebAdmin[382]
Account Editor » WorldClient e WebAdmin[347]

4.3.2.2 SSL / HTTPS

Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). Il protocollo SSL, sviluppato da Netscape Communications Corporation, è il metodo standard per la protezione delle comunicazioni Web server/client e offre funzioni per l'autenticazione server, la crittografia dei dati e

l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare WebAdmin per l'utilizzo di HTTPS si trovano nella schermata SSL/HTTPS, disponibile in "Impostazioni » Web, Sincronizzazione e Servizi IM » WebAdmin (configurazione Web)". Per praticità, tali impostazioni sono presenti anche in "Sicurezza» Impostazioni sicurezza » SSL e TLS » WebAdmin".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e certificati** 311

Questa schermata è valida per WebAdmin solo quando si utilizza il server Web incorporato di MDaemon. Se si configura WebAdmin per l'esecuzione con altri server Web quali IIS, queste opzioni non sono disponibili. Il supporto per SSL/HTTPS dovrà essere configurato con gli strumenti offerti dal server Web utilizzato.

Tipi di connessioni accettate

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a WebAdmin. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in WebAdmin, ma non si desidera imporre agli utenti di WebAdmin l'utilizzo di HTTPS. WebAdmin rimane in attesa di connessioni sulla *porta HTTPS* indicata di seguito, ma risponde anche alle normali connessioni HTTP sulla porta TCP di WebAdmin definita nella schermata Server Web 145 di WebAdmin (configurazione Web).

Solo HTTPS
Scegliere questa opzione se si desidera richiedere l'utilizzo di HTTPS al momento della connessione a WebAdmin. Se si attiva questa opzione, WebAdmin risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da WebAdmin per le connessioni SSL. La porta SSL predefinita è 443. Se si utilizza la porta predefinita, per le connessioni HTTPS non è necessario includere il numero della porta nell'URL di WebAdmin (vale a dire, "https://esempio.com" è equivalente a "https://esempio.com:443").

Questa porta è diversa dalla porta di WebAdmin definita nella scheda Server Web 145 della schermata WebAdmin (configurazione Web). Se consentite, le connessioni HTTP a WebAdmin devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

Certificati

Questa casella consente di visualizzare i certificati SSL. Per definire il certificato da utilizzare in WebAdmin, selezionarlo dall'elenco. Fare doppio clic sul certificato per aprire la finestra di dialogo Certificato che consente di visualizzarne o modificarne i dettagli.

MDaemon non consente l'utilizzo di più certificati per WebAdmin. Tutti i domini devono condividere un unico certificato. Qualora sia disponibile più di un dominio, inserire i nomi di tali domini e di quelli che si intende utilizzare per accedere a WebAdmin nel campo denominato "*Nomi host alternativi (separare le voci con una virgola)*" descritto di seguito.

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wa.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Il supporto di più certificati non è disponibile. Tutti i domini devono condividere un unico certificato. Qualora per le connessioni degli utenti esistano nomi host alternativi, inserire i nomi dei domini separati da virgole nel caso in cui si intenda applicare il certificato anche ai nomi alternativi. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Crea certificato
Dopo aver inserito tutte le informazioni nei controlli descritti in precedenza, per creare il certificato fare clic su questo pulsante.

Riavvia server Web
Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare i nuovi certificati, è necessario riavviare il server Web.

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere:

Esecuzione di WebAdmin con IIS 150
SSL e certificati 311
Creazione e uso dei certificati SSL 320

Per ulteriori informazioni su WebAdmin, vedere:

Configurazione remota 144
WebAdmin » Server Web 145
Valori predefiniti del nuovo account » WorldClient e WebAdmin 382
Account Editor » WorldClient e WebAdmin 347

4.3.2.3 Esecuzione di WebAdmin con IIS

Poiché in WebAdmin è incorporato un server Web, Internet Information Server (IIS) non è richiesto. WebAdmin supporta comunque IIS e può pertanto funzionare come DLL ISAPI.

Per configurare il funzionamento con IIS 5:

1. Interrompere l'esecuzione di WebAdmin. A questo scopo, fare clic con il pulsante destro del mouse sulla voce WebAdmin di *Server* nel riquadro sinistro della GUI di MDaemon e fare clic su **Attiva/Disattiva.**

2. Aprire il programma di gestione IIS mediante **Start→Impostazioni→Pannello di controllo→ Strumenti di amministrazione→Gestione servizio Internet.**

3. Fare clic con il pulsante destro del mouse su **Sito Web predefinito** e selezionare **Nuovo →Directory virtuale**.

4. Attenersi alla procedura guidata che illustra passo dopo passo il processo di creazione di una directory virtuale. Di seguito vengono suggeriti nomi e percorsi per i dati da digitare nella procedura guidata, che possono comunque variare in base all'installazione di MDaemon e alla posizione di WebAdmin.

    a. Alias: "`WebAdmin`". Scegliere **Avanti**.
    b. Directory: "`c:\mdaemon\webadmin\templates`". Scegliere **Avanti**.
    c. Fare clic su **Avanti**.
    d. Fare clic su **Fine**.

5. Impostare le autorizzazioni di esecuzione su **Solo script**.

6. Impostare il livello di protezione dell'applicazione su **Basso (Processo IIS)**.

7. Fare clic sul pulsante **Configurazione** nella sezione Impostazioni applicazione della scheda Directory virtuale.

8. Nella scheda **Mapping**, fare clic su **Aggiungi**.

9. Nel campo **Eseguibile** inserire "`c:\mdaemon\webadmin\templates\WebAdmin.dll`". Nota: nel campo non possono essere inseriti spazi. Se il percorso contiene uno spazio, è necessario convertirlo nel formato 8.3. Il comando `dir /x` consente di visualizzare il nome del file o della directory nel formato 8.3.

10. Nel campo **Estensione** inserire "`.wdm`" e selezionare il pulsante di opzione per **Tutti i verbi**.

11. Fare clic sulla casella **Modulo script**.

12. Fare clic su **OK**.

13. Se si desidera, rimuovere le altre mappature, quindi scegliere **OK**.

14. Nella scheda **Documenti** aggiungere `login.wdm` come documento predefinito e rimuovere tutte le altre voci dall'elenco.

15. In MDaemon, passare a **Impostazioni→Web, Sincronizzazione e Servizi IM→WebAdmin** e fare clic su **WebAdmin utilizza server Web esterni**.

16. In **URL WebAdmin** inserire "`/WebAdmin/login.wdm`".

17. Fare clic su **OK**.

Per configurare il funzionamento con IIS 6:

Creare un nuovo pool di applicazioni per WebAdmin:

1. Interrompere l'esecuzione di WebAdmin. A questo scopo, fare clic con il pulsante destro del mouse sulla voce WebAdmin di *Server* nel riquadro sinistro della GUI di MDaemon e fare clic su **Attiva/Disattiva**.

2. Aprire il programma di gestione IIS mediante **Start→Impostazioni→Pannello di controllo→ Strumenti di amministrazione→Gestione servizio Internet**.

3. Fare clic con il pulsante destro del mouse su **Pool applicazioni**.

4. Fare clic su **Nuovo→Pool applicazioni**.

5. Nel campo dell'ID del pool di applicazioni inserire "`Alt-N`" e fare clic su **OK**.

6. Fare clic con il pulsante destro del mouse su **Alt-N**.

7. Scegliere **Proprietà**.

8. Fare clic sulla scheda **Prestazioni.**

9. Deselezionare "**Chiudi processi di lavoro dopo un periodo di inattività di**" e "**Limite massimo per la coda di richieste al kernel**".

10. Fare clic sulla scheda **Identità.**

11. Nell'elenco a discesa Predefinito, scegliere **Sistema locale**.

12. Fare clic su **OK**.

Creare una directory virtuale per WebAdmin:

1. Aprire il programma di gestione IIS mediante **Start→Impostazioni→Pannello di controllo→** Strumenti di amministrazione (Gestione servizio Internet).

2. Fare clic con il pulsante destro del mouse sul sito Web, quindi selezionare Nuovo (Directory virtuale).

3. Specificare un alias per la directory virtuale (ad esempio "WebAdmin").

4. Nel campo Percorso, digitare il percorso della directory dei modelli di WebAdmin, ad esempio "C:\Programmi\Alt-N Technologies\WebAdmin\Templates".

5. Lasciare selezionate le opzioni Lettura ed Esecuzione script.

6. Completare la procedura guidata e fare clic con il pulsante destro del mouse sulla directory virtuale creata.

7. Selezionare Proprietà.

8. Nella scheda Home Directory modificare il pool di applicazioni in Alt-N.

9. Fare clic sul pulsante Configurazione.

10. Scegliere Aggiungi per aggiungere una mappatura con estensione ISAPI.

11. Nel campo Eseguibile inserire il percorso del file WebAdmin.dll. Ad esempio, "C:\Programmi\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll".

12. Nel campo Estensione inserire ".wdm"

13. Selezionare le caselle **Modulo script** e **Verifica esistenza file**.

14. Fare clic su **OK**.

15. Se si desidera, rimuovere le altre mappature, quindi scegliere **OK**.

16. Selezionare la scheda **Documenti.**

17. Verificare che l'opzione **Abilita pagina contenuto predefinita** sia selezionata.

18. Accertarsi che l'elenco includa solo la voce "`login.wdm`".

19. Fare clic su **OK** e uscire dalla finestra di dialogo delle proprietà della directory virtuale.

Aggiungere `.WDM` all'elenco delle estensioni Web consentite:

1. Fare clic sulla cartella **Estensioni servizi Web** di IIS MMC.

2. Fare clic su **Aggiungi nuova estensione servizio Web**.

3. Nel campo Estensione inserire "`WebAdmin`".

4. Fare clic su **Aggiungi**, quindi selezionare l'estensione ISAPI WebAdmin. Ad esempio: `C:\Programmi\Alt-N Technologies\WebAdmin\Templates\WebAdmin.dll`.

5. Selezionare **Imposta stato estensione su consentito**.

6. Fare clic su **OK**.

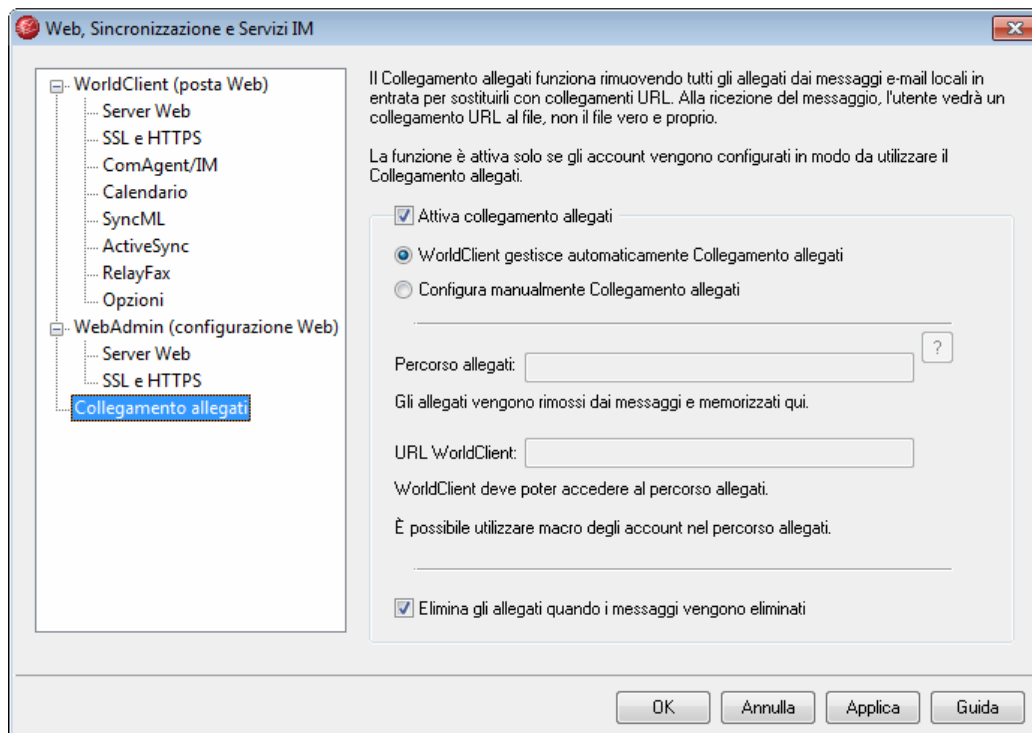
7. In MDaemon, passare a **Impostazioni→Web, Sincronizzazione e Servizi IM→WebAdmin** e fare clic su **WebAdmin utilizza server Web esterni**.

8. In **WebAdmin URL** inserire "/`WebAdmin/login.wdm`".

9. Fare clic su **OK**.

Per ulteriori informazioni su WebAdmin, vedere:

Configurazione remota 144
WebAdmin » Server Web 145
WebAdmin » HTTPS 147
Valori predefiniti del nuovo account » WorldClient e WebAdmin 382
Account Editor » WorldClient e WebAdmin 347

4.3.3 Collegamento degli allegati

La funzione Collegamento allegati (Impostazioni » Web, Sincronizzazione e Servizi IM » Collegamento allegati) consente di rimuovere tutti gli allegati dai messaggi di posta elettronica in arrivo, di memorizzarli nella posizione indicata e di inserire collegamenti URL ai file nei messaggi dai quali sono stati estratti. I destinatari possono quindi selezionare i collegamenti per scaricare i file. Grazie a questa funzione, è possibile velocizzare l'elaborazione della posta elettronica, in particolare quando gli utenti ricevono messaggi o sincronizzano le proprie cartelle di posta, perché vengono eliminati gli allegati di grandi dimensioni. La funzione offre inoltre una maggiore sicurezza e un accresciuto livello di protezione perché gli allegati possono essere memorizzati in una posizione centralizzata, soggetta al controllo dell'amministratore, e non vengono scaricati direttamente da client di posta elettronica che potrebbero eseguirli automaticamente. Selezionando l'opzione "*WorldClient gestisce automaticamente Collegamento allegati*", i percorsi dei file e dell'URL di WorldClient vengono gestiti automaticamente. Con la gestione manuale di Collegamento allegati, è possibile specificare la posizione nella quale memorizzare i file e renderla dinamica mediante particolari macro. Per un corretto funzionamento di Collegamento allegati, è necessario aver attivato tale funzione a livello globale mediante l'opzione di questa schermata e aver configurato espressamente ogni account desiderato nella schermata Posta e allegati 345 di Account Editor. I collegamenti inseriti da MDaemon nei messaggi non contengono i percorsi diretti dei file agli allegati. Contengono invece un identificativo univoco (GUID) utilizzato dal server per mappare il file al percorso effettivo. La mappatura dei GUID è memorizzata nel file `AttachmentLinking.dat`.

Attiva collegamento allegati
Questa casella di controllo consente di attivare Collegamento allegati per tutti gli account espressamente configurati a questo scopo nella schermata Posta e allegati

345 di Account Editor. Quando si attiva l'opzione globale, viene richiesto se si desidera anche attivare l'opzione specifica per tutti gli account di MDaemon. Se si seleziona "Sì", Collegamento allegati viene abilitato per tutti gli account e viene attivata anche l'opzione corrispondente di Valori predefiniti del nuovo account 377. Se si sceglie "No", la funzione Collegamento allegati viene abilitata, ma sarà necessario attivare manualmente l'estrazione degli allegati per ogni account. Dopo aver abilitato Collegamento allegati, è necessario che il server WorldClient rimanga attivo.

WorldClient gestisce automaticamente Collegamento allegati
Questa è l'opzione predefinita quando si attiva Collegamento allegati. Con questa opzione, WorldClient gestisce automaticamente Collegamento allegati. I file estratti vengono memorizzati in: "...\MDaemon\Attachments\$DOMAIN$\$MAILBOX$\".

Configura manualmente Collegamento allegati
Questa opzione consente di indicare la cartella nella quale memorizzare gli allegati. Selezionando l'opzione, è necessario indicare sia il percorso degli allegati che l'URL di WorldClient.

Percorso allegati
Questa casella di testo consente di indicare la cartella in cui memorizzare gli allegati estratti. È possibile impostare un percorso statico o utilizzare le macro di modello 381 e script 390 per rendere il percorso dinamico. Ad esempio, con "$ROOTDIR$\Attachments\$DOMAIN$\" tutti gli allegati vengono raggruppati in una sottocartella denominata in base al dominio cui appartiene l'utente, contenuta in un'altra sottocartella denominata "Attachments" che si trova nella cartella principale di MDaemon, in genere C:\MDaemon\. Di conseguenza, nel caso di "franco@esempio.com" già citato, gli allegati estratti vengono collocati nella sottocartella "C:\MDaemon\Attachments\esempio.com\." Per definire ulteriormente la posizione di memorizzazione degli allegati, è possibile aggiungere la macro di modello "$MAILBOX$" all'esempio precedente. In tal modo, i file di Franco verranno memorizzati nella sottocartella di "\esempio.com\" denominata "Franco." Il nuovo percorso pertanto sarà: "C:\MDaemon\Attachments\esempio.com\Franco\."

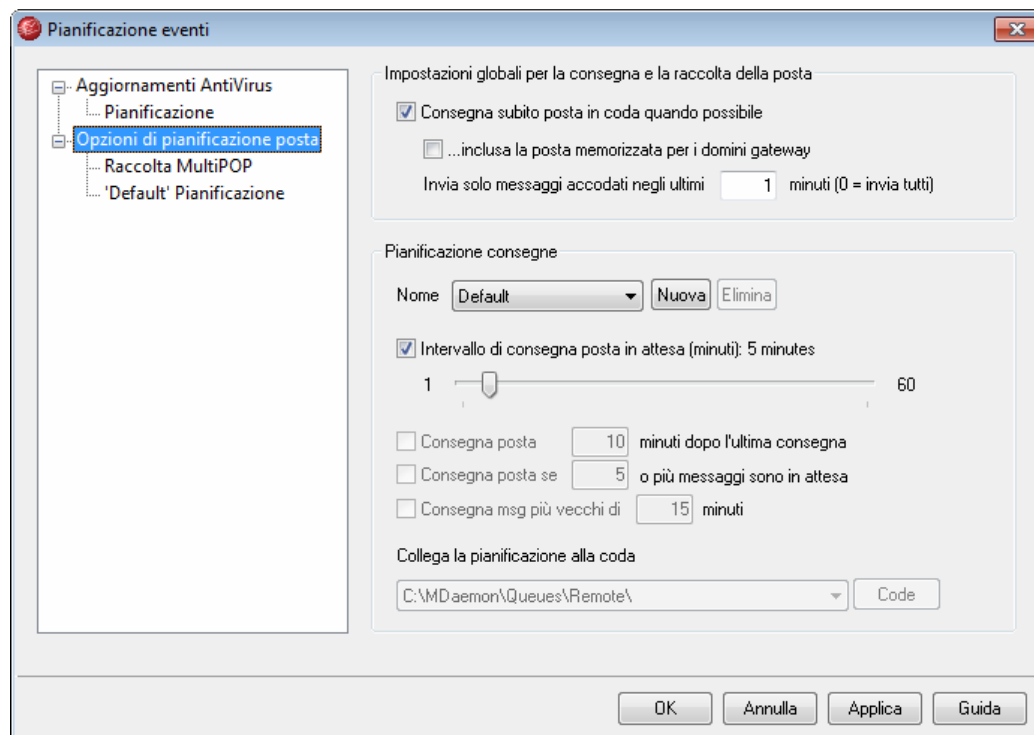
URL di WorldClient
Immettere l'URL di WorldClient, ad esempio "http://mail.example.com:3000/WorldClient.dll". MDaemon utilizza tale URL per inserire i collegamenti nei messaggi dai quali sono estratti gli allegati.

Elimina gli allegati quando i messaggi vengono eliminati
Selezionare questa opzione se si desidera eliminare dal server gli allegati estratti quando il messaggio cui sono associati viene eliminato. Prestare attenzione prima di attivare questa opzione, perché se viene attivata e un utente raccoglie la posta con un client POP3 non configurato in modo da lasciare i messaggi nel server, tutti gli allegati estratti andranno persi. Se questa opzione **non** è attivata non si perderà alcun allegato, ma è possibile che i file degli allegati non più necessari occupino inutilmente una notevole quantità di spazio su disco. Tutti i client POP consentono di lasciare i messaggi nel server.

Vedere:

[Posta e allegati](345)
[Macro dei modelli](381)
[Macro degli script](390)

4.4 Pianificazione eventi

4.4.1 Opzioni di pianificazione posta

Fare clic su Impostazioni » Dominio predefinito/server » Pianificazione eventi per aprire Pianificazione eventi di MDaemon. La sezione Opzioni pianificazione posta di questa finestra di dialogo consente di pianificare gli eventi di pianificazione della posta remota di MDaemon, in modo semplice o avanzato, a seconda delle esigenze. È possibile utilizzare un contatore per elaborare la posta a intervalli regolari oppure pianificare il momento esatto di consegna e di raccolta della posta mediante le schermate di pianificazione159. È inoltre possibile impostare delle condizioni che attivano l'elaborazione della posta a prescindere dagli orari pianificati, ad esempio al raggiungimento di un determinato numero di messaggi in attesa di essere consegnati oppure alla scadenza del tempo specificato. È possibile creare pianificazioni personalizzate che possono essere assegnate a code di posta remote personalizzate. Le pianificazioni personalizzate consentono di impostare pianificazioni differenti in base ai diversi tipi di messaggio. Ad esempio, è possibile creare pianificazioni relative ai messaggi di grandi dimensioni, ai messaggi indirizzati alle liste di distribuzione, ai messaggi provenienti da domini specifici e così via.

Se si è installato SecurityPlus per MDaemon 211, utilizzare la sezione Aggiornamenti AntiVirus 163 di Pianificazione eventi per pianificare la frequenza con la quale MDaemon verificherà l'eventuale esistenza di aggiornamenti AntiVirus.

Impostazioni globali per la consegna e la raccolta della posta

Consegna subito posta in coda quando possibile
Se questa opzione è abilitata, quando un messaggio viene ricevuto e accodato per la consegna remota, anziché attivare l'elaborazione della posta dopo il successivo intervallo pianificato o a seguito di un altro evento, MDaemon elabora e consegna immediatamente tutta la posta remota inserita nella coda nel periodo di tempo indicato nell'opzione *Invia solo messaggi accodati negli ultimi XX minuti*.

...inclusa la posta memorizzata per i domini gateway
Selezionare questa casella di controllo se si desidera che i messaggi per i gateway di dominio vengano consegnati immediatamente. Questa opzione si applica, tuttavia, solo ai gateway per i quali sia stata abilitata l'opzione *Consegna i messaggi memorizzati ogni volta che MDaemon elabora la posta remota* nella schermata Gateway 460 di Gateway Editor.

Invia solo messaggi accodati negli ultimi XX minuti (0=invia tutti)
Questa opzione consente di specificare il tempo di attesa nella coda dei messaggi prima dell'esecuzione dell'opzione *Consegna subito posta in coda quando possibile*. Quando tale opzione attiva l'elaborazione della posta remota, MDaemon elabora solo i messaggi inseriti nella coda dal numero di minuti specificato anziché elaborare indiscriminatamente tutti i messaggi presenti nella coda. L'intera coda viene comunque elaborata quando si preme uno dei pulsanti *Elabora coda...* della barra degli strumenti o quando un normale evento di pianificazione attiva l'elaborazione della posta remota. L'impostazione predefinita di questa opzione è di un minuto. Se si desidera elaborare l'intera coda a ogni attivazione dell'elaborazione della posta remota è possibile impostare l'opzione su 0. Tuttavia, questa impostazione non è consigliabile in quanto molto meno efficiente.

Le opzioni descritte in precedenza vengono applicate solo alla pianificazione predefinita (Default) e non sono disponibili per le pianificazioni personalizzate. Vedere l'opzione *Nome* descritta successivamente.

Nome
Utilizzare questa casella di riepilogo a discesa per selezionare la pianificazione da modificare. La pianificazione Default viene utilizzata per le code di posta normali e remote, nonché per la posta raccolta mediante DomainPOP e MultiPOP. Nel caso di configurazioni che includano servizi di accesso remoto (RAS), la pianificazione Default viene utilizzata anche per i domini LAN, ossia per i domini remoti definiti come residenti nella rete locale in uso e che, di conseguenza, non prevedono l'uso di connessioni RAS. È possibile assegnare altre pianificazioni alle code di posta remota personalizzate. I messaggi possono essere instradati automaticamente alle code

personalizzate 488 mediante Filtro contenuti 212. Dopo aver completato la modifica di una pianificazione, fare clic su OK oppure selezionare un'altra pianificazione da modificare. Se si apportano modifiche a una pianificazione e si seleziona un'altra pianificazione, viene visualizzata una casella di conferma che richiede di salvare o annullare le modifiche apportate prima di passare alla pianificazione desiderata.

Nuova
Fare clic su questa opzione per creare una nuova pianificazione. Viene aperta una casella per l'inserimento del nome. Dopo aver indicato il nome della pianificazione, nel menu di sinistra viene creata una schermata Pianificazione 159 apposita. In questa schermata è possibile indicare gli orari di pianificazione.

Elimina
Per eliminare una pianificazione personalizzata, selezionarla nell'elenco a discesa *Nome*, quindi fare clic su *Elimina*. Viene visualizzata una finestra che richiede di confermare l'eliminazione. L'eliminazione di una pianificazione personalizzata non determina l'eliminazione delle code remote personalizzate o delle regole di Filtro contenuti associate alla pianificazione. Tuttavia, se si elimina una coda personalizzata, verranno eliminate anche le pianificazioni personalizzate e le regole di Filtro contenuti associate alla coda.

Intervallo di consegna posta in attesa (minuti):
Selezionare questa casella di controllo e spostare il cursore verso destra o sinistra per specificare l'intervallo di tempo tra ogni sessione di elaborazione della posta. Il conteggio alla rovescia può essere impostato su un valore compreso tra 1 e 60 minuti. Allo scadere del tempo stabilito, MDaemon elaborerà la posta remota e il conto alla rovescia verrà reimpostato sul valore originale. Se la casella di controllo è deselezionata, gli intervalli di elaborazione della *posta remota*saranno determinati dalle altre opzioni di pianificazione.

Consegna posta XX minuti dopo l'ultima consegna
Questa opzione consente di indicare l'esecuzione a intervalli di tempo regolari delle sessioni di elaborazione della posta remota successive all'ultima sessione, indipendentemente dall'evento che ha avviato quest'ultima. A differenza degli intervalli fissi stabiliti con l'impostazione di orari specifici o utilizzando la barra di scorrimento *Intervallo di consegna posta in attesa*, con questa opzione l'intervallo orario viene reimpostato ad ogni elaborazione della posta.

Consegna posta se XX o più messaggi sono in attesa
Se si abilita questa opzione, MDaemon avvia una sessione di posta quando il numero di messaggi in attesa nella coda remota è uguale o superiore al valore specificato in questo campo. Queste sessioni di posta sono aggiuntive rispetto a tutte le altre normalmente pianificate.

Consegna msg più vecchi di XX minuti
Se questa casella è abilitata, MDaemon avvia sempre una sessione di posta quando un messaggio è rimasto nella coda per il numero di minuti specificato. Queste sessioni sono aggiuntive rispetto a tutte le altre normalmente pianificate.

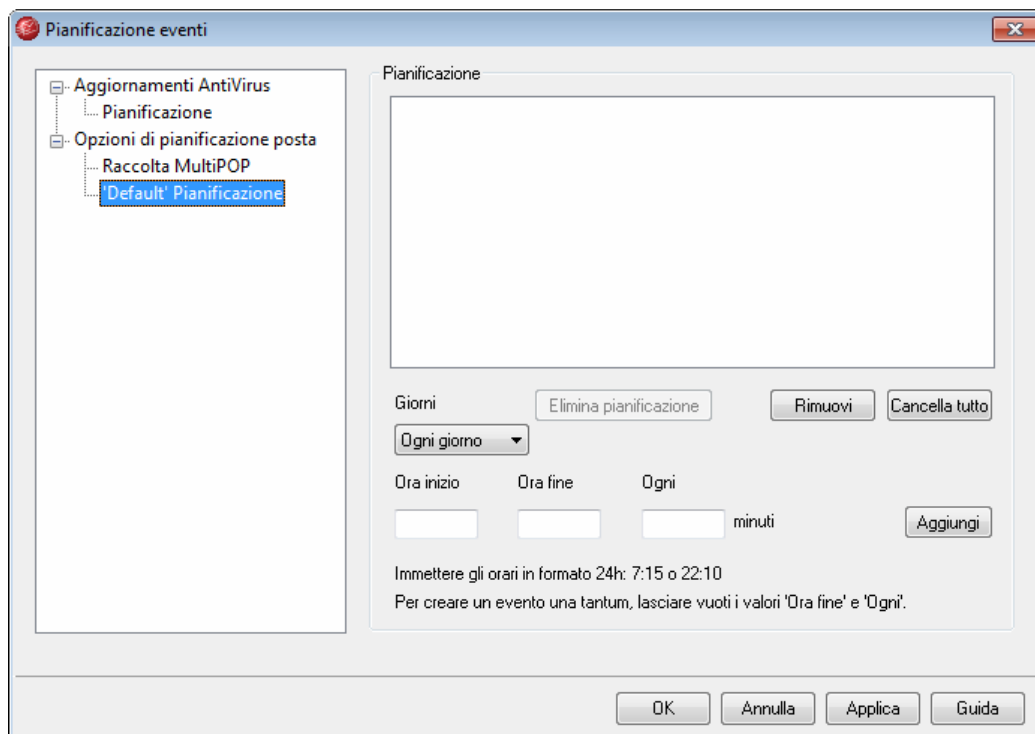
Code

Collega la pianificazione alla coda
Utilizzare questa opzione per associare la pianificazione selezionata a una specifica coda di posta remota personalizzata. Mediante Filtro contenuti sarà quindi possibile creare regole che consentano di inserire alcuni messaggi nella coda personalizzata. Se, ad esempio, si desidera pianificare la consegna in un determinato momento dei messaggi delle liste di distribuzioni indirizzati a destinatari remoti, è possibile creare una coda personalizzata associata a tali messaggi, definire una regola che collochi tutti i messaggi di questo tipo nella coda personalizzata e creare una pianificazione personalizzata da assegnare alla coda in questione.

Code
Questo pulsante consente di aprire la schermata Code personalizzate 488, per la creazione di code remote personalizzate da utilizzare con Pianificazione eventi.

Vedere:

Pianificazione della posta 159
Aggiornamenti AntiVirus 163

4.4.1.1 Pianificazione della posta

Ogni pianificazione della posta corrisponde a una pianificazione con lo stesso nome presente nell'elenco a discesa *Nome* della schermata Opzioni di pianificazione posta 156. Le singole pianificazioni della posta consentono di indicare gli orari in cui, per quella

pianificazione, si verificherà l'elaborazione remota della posta. Le pianificazioni della posta sono situate nel percorso: Impostazioni » Pianificazione eventi » Opzioni di pianificazione posta » 'NomePianificazione' Pianificazione.

Pianificazione

Elimina pianificazione
Questo pulsante consente di eliminare la pianificazione della posta personalizzata. La pianificazione viene eliminata e le relative voci vengono rimosse dall'elenco a discesa *Nome* della schermata Opzioni di pianificazione posta 156. Quando si seleziona questo pulsante, viene aperta una finestra con una richiesta di conferma. Questa opzione è disponibile solo per le pianificazioni personalizzate, mentre non è possibile eliminare la pianificazione Default.

Rimuovi
Per rimuovere una voce dall'elenco, selezionarla e fare clic su questo pulsante.

Cancella tutto
Con questo pulsante vengono rimosse tutte le voci della pianificazione.

Creazione di eventi pianificati

Giorni
Quando si crea un nuovo evento di pianificazione, è necessario selezionare innanzitutto in quali giorni si desidera che si verifichi. È possibile selezionare: tutti i giorni, giorni feriali (da lunedì a venerdì), fine settimana (sabato e domenica) oppure determinati giorni della settimana.

Ora inizio
Inserire l'ora in cui si desidera che l'evento abbia inizio. Il formato dell'orario deve essere di 24 ore, dalle 00:00 alle 23:59. Se si desidera che l'evento sia isolato anziché ricorrente, inserire solo questo valore, lasciando vuote le opzioni *Ora fine* e *Ogni*.

Ora fine
Inserire l'ora in cui si desidera che l'evento si concluda. Il formato dell'orario deve essere di 24 ore, dalle 00:01 alle 23:59 e il valore deve essere successivo a quello di *Ora inizio*. Se, ad esempio, il valore di *Ora inizio* è "10:00", questo valore deve essere compreso tra le "10:01" e le "23:59". Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Ogni [xx] minuti
Indica l'intervallo orario in cui la posta verrà elaborata tra gli orari *Ora inizio* e *Ora fine* indicati. Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Aggiungi
Dopo aver indicato i *Giorni* e l'*Ora inizio*, l'*Ora fine* facoltativa e il valore *Ogni*, aggiungere l'evento alla pianificazione con questo pulsante.

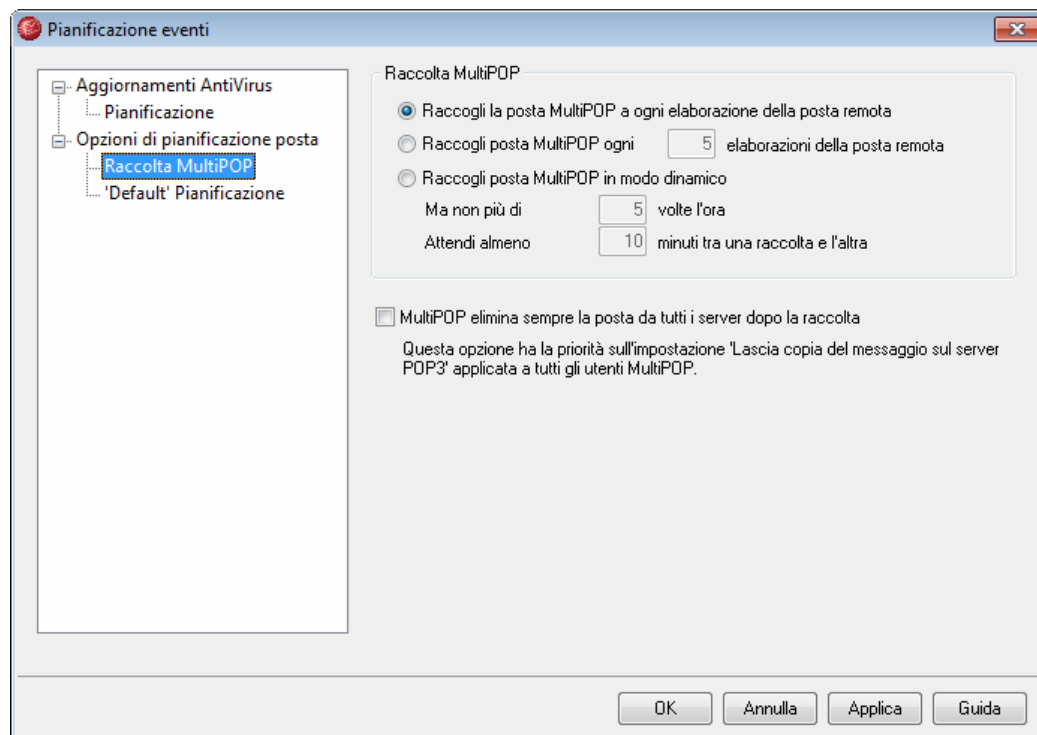
In base alle diverse esigenze, per controllare gli intervalli di elaborazione della posta può essere sufficiente utilizzare le opzioni di pianificazione semplici della schermata Opzioni di pianificazione posta156. Ad esempio, non è necessario stabilire una pianificazione specifica con eventi per ogni minuto di ogni giorno quando è sufficiente impostare la barra di scorrimento di Opzioni di pianificazione posta su intervalli di un minuto per ottenere lo stesso risultato. D'altra parte, per specificare intervalli di elaborazione superiori a 60 minuti, anche solo per alcuni giorni, è possibile avvalersi di una combinazione di opzioni di pianificazione e di orari specifici.

Vedere:

Opzioni di pianificazione posta 156

Aggiornamenti AntiVirus 163

Aggiornamenti Antispam 263

4.4.1.2 Raccolta MultiPOP

Raccolta MultiPOP

Raccogli la posta MultiPOP a ogni elaborazione della posta remota

Scegliere questa opzione per consentire a MDaemon di raccogliere tutta la posta MultiPOP367 a ogni elaborazione della posta remota.

Raccogli posta MultiPOP ogni XX elaborazioni della posta remota
Scegliere questa opzione e specificare un valore nel campo per raccogliere la posta MultiPOP con una frequenza inferiore a quella di elaborazione della posta remota. Il valore indica per quante volte la posta remota viene elaborata prima della raccolta della posta MultiPOP.

Raccogli posta MultiPOP in modo dinamico
Scegliere questa opzione per raccogliere i messaggi MultiPOP in modo dinamico. Di norma, la posta MultiPOP viene raccolta per tutti gli utenti contemporaneamente a ogni intervallo di elaborazione remota della posta oppure ogni *x* intervalli. Nella raccolta dinamica, i messaggi MultiPOP vengono raccolti per ogni singolo utente quando questi controlla la propria posta mediante POP, IMAP o WorldClient. Tuttavia, poiché la raccolta MultiPOP viene attivata quando l'utente controlla la posta, gli eventuali nuovi messaggi MultiPOP raccolti non risulteranno visibili all'utente finché questi non controlla *nuovamente* la posta. Sarà quindi necessario controllare la posta due volte per visualizzare i nuovi messaggi MultiPOP, la prima per attivare MultiPOP e la seconda per visualizzare la posta raccolta.

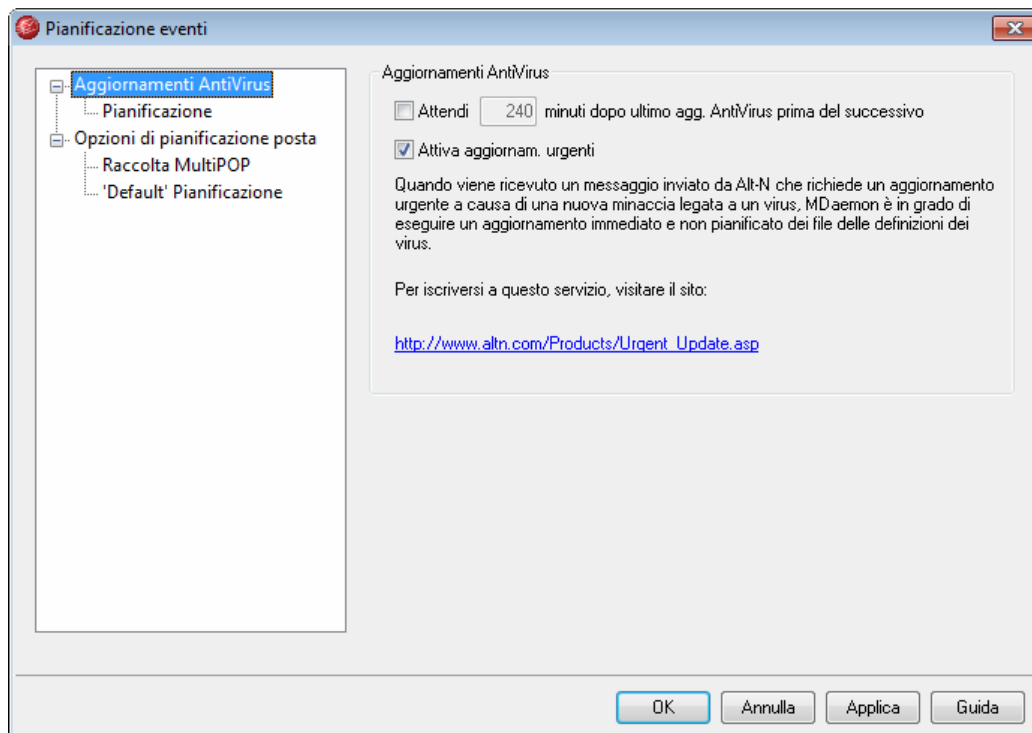
Ma non più di XX volte all'ora
Per ridurre ulteriormente il carico generato dall'uso frequente del metodo MultiPOP, è possibile avvalersi di questo comando e specificare quanto volte in un'ora deve essere raccolta la posta MultiPOP per ogni utente.

Attendi almeno XX minuti tra una raccolta e l'altra
Questa opzione è utile per ridurre il carico del server di posta, poiché limita la frequenza con cui i messaggi MultiPOP possono essere raccolti per ogni utente. L'opzione consente di impostare la raccolta della posta MultiPOP per utente in base a intervalli specifici, espressi in minuti. Specificare il numero di minuti che si desidera trascorrano prima che all'utente sia consentito di controllare di nuovo la posta MultiPOP.

MultiPOP elimina sempre la posta da tutti i server dopo la raccolta
Selezionare questa casella di controllo per eseguire l'override dell'opzione *Lascia una copia del messaggio sul server POP* presente nella schermata MultiPOP 367 di Account Editor. Una volta raccolti, i messaggi verranno eliminati da ciascun server MultiPOP.

Vedere:

MultiPOP 367

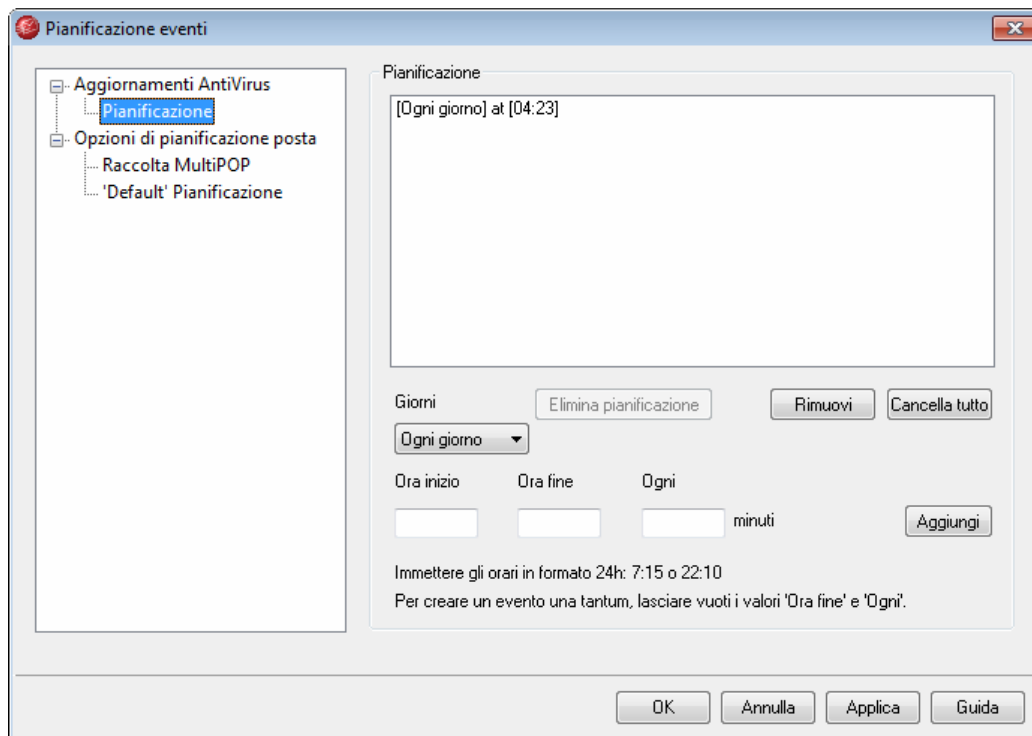
4.4.2 Aggiornamenti AntiVirus

Aggiornamenti AntiVirus

Attendi XX minuti dopo ultimo agg. AntiVirus prima del successivo
Selezionare questa casella di controllo e specificare il numero di minuti che devono trascorrere prima che SecurityPlus per MDaemon verifichi se sono disponibili nuovi aggiornamenti delle definizioni dei virus. Si noti che in realtà si tratta del numero di minuti per cui SecurityPlus *tenterà* di attendere dopo l'ultima ricerca di un aggiornamento, indipendentemente dal fatto che quest'ultima sia stata eseguita manualmente o sia stata attivata dalla funzione di pianificazione. Gli aggiornamenti eseguiti manualmente o da un'utilità di pianificazione hanno la precedenza su questa impostazione. Di conseguenza, al verificarsi di uno di questi aggiornamenti, questo contatore viene azzerato. In altri termini, se l'opzione è impostata per verificare la disponibilità di aggiornamenti ogni 240 minuti e dopo 100 minuti si cerca manualmente un aggiornamento, il contatore verrà reimpostato su 240 minuti.

Aggiornamenti urgenti

Attiva aggiornamenti urgenti
Questa casella di controllo consente di attivare la funzione relativa agli aggiornamenti urgenti. Se la funzione è abilitata, SecurityPlus per MDaemon si connetterà e scaricherà l'aggiornamento urgente non appena ne viene notificata la disponibilità. Per ricevere questi messaggi, è necessario aggiungere il proprio dominio al sistema Aggiornamenti urgenti di altn.com.

Per utilizzare questa funzione è necessario avere abilitato l'opzione "*Verifica firme DKIM*" della schermata Verifica DKIM289.

4.4.2.1 Pianificazione degli aggiornamenti AntiVirus

La pianificazione degli aggiornamenti AntiVirus consente di indicare orari specifici nei quali SecurityPlus211 possa controllare gli aggiornamenti di AntiVirus. La pianificazione è disponibile in: Impostazioni » Pianificazione eventi » Aggiornamenti AntiVirus » Pianificazione.

Pianificazione

Rimuovi
Per rimuovere un evento dall'elenco, selezionare la voce desiderata e fare clic su questo pulsante.

Cancella tutto
Con questo pulsante vengono rimosse tutte le voci della pianificazione.

Creazione di eventi pianificati

Giorni
Quando si crea un nuovo evento pianificato, è necessario selezionare innanzitutto in quali giorni si desidera che si verifichi il controllo dell'aggiornamento. È possibile

selezionare: tutti i giorni, giorni feriali (da lunedì a venerdì), fine settimana (sabato e domenica) oppure determinati giorni della settimana.

Ora inizio
Inserire l'ora in cui si desidera che abbia inizio il controllo degli aggiornamenti. Il formato dell'orario deve essere di 24 ore, dalle 00:00 alle 23:59. Se si desidera che l'evento sia isolato anziché ricorrente, inserire solo questo valore, lasciando vuote le opzioni *Ora fine* e *Ogni*.

Ora fine
Inserire l'ora in cui si desidera che termini il controllo degli aggiornamenti. Il formato dell'orario deve essere di 24 ore, dalle 00:01 alle 23:59 e il valore deve essere successivo a quello di *Ora inizio*. Se, ad esempio, il valore di *Ora inizio* è "10:00", questo valore deve essere compreso tra le "10:01" e le "23:59". Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Ogni [xx] minuti
Indica l'intervallo orario in cui SecurityPlus controllerà gli aggiornamenti tra gli orari *Ora inizio* e *Ora fine* indicati. Se si desidera che l'evento sia isolato e non ricorrente, lasciare questa opzione vuota.

Aggiungi
Dopo aver indicato i *Giorni* e l'*Ora inizio*, l'*Ora fine* facoltativa e il valore *Ogni*, aggiungere l'evento alla pianificazione con questo pulsante.

Vedere:

Aggiornamenti AntiVirus 232
AntiVirus 232
Utilità di aggiornamento AntiVirus 235

4.5 BlackBerry

4.5.1 BES BlackBerry

MDaemon Pro è dotato di un server BES integrato e personalizzato, ideato espressamente per la distribuzione e l'utilizzo con MDaemon. Il server BES consente agli utenti di sincronizzare i messaggi di posta elettronica, il calendario e altri dati PIM (Personal Information Management) di MDaemon/WorldClient con gli smartphone BlackBerry. BES consente inoltre di impostare criteri di sicurezza sui dispositivi degli utenti e perfino di cancellare i dati da un dispositivo in caso di smarrimento o di furto.

Le funzionalità BES di MDaemon sono elencate di seguito.

- Nessuna necessità di client di sincronizzazione di terze parti. I dati dei singoli utenti vengono sincronizzati mediante il software già presente in tutti i dispositivi BlackBerry.
- I messaggi di posta elettronica di MDaemon/WorldClient, incluse le cartelle di

posta, vengono sincronizzati con il dispositivo in entrambe le direzioni. Pertanto le operazioni di lettura, spostamento, eliminazione e così via della posta, sono sincronizzate sia sul dispositivo che sul server ovunque si siano verificate.

- Sincronizzazione bidirezionale del calendario. Se ad esempio si crea un nuovo appuntamento, si imposta un promemoria o si modifica un appuntamento sul dispositivo o in WorldClient, l'operazione viene sincronizzata su entrambi.
- Sincronizzazione bidirezionale delle attività e delle note.
- Ricerca nella rubrica globale.
- Pianificazione della disponibilità (Free/Busy).
- Supporto limitato dei criteri dei dispositivi BlackBerry che consente l'impostazione di criteri quali: richiesta della password, scadenza della password, crittografia dei file multimediali e altro ancora.
- Impostazione di criteri diversi per i singoli domini o utenti.
- Modifica remota della password e blocco del dispositivo.
- Cancellazione dei dati dal dispositivo in caso, ad esempio, di smarrimento o furto.
- Opzioni di backup e di ripristino del database BES.

Le principali opzioni BES di MDaemon si trovano in: Impostazioni » BlackBerry... » BES BlackBerry, mentre le opzioni specifiche per gli account si trovano nella schermata BES BlackBerry 350 di Account Editor.

Finestra di dialogo BlackBerry

La sezione BES BlackBerry della finestra di dialogo BlackBerry include le seguenti schermate:

Stato 169: questa schermata consente di attivare o disattivare BES e di visualizzare lo stato dei diversi componenti e servizi. Vengono visualizzate anche le informazioni univoche sul protocollo SRP (Server Routing Protocol), inclusi l'ID e la chiave.

Criteri 170: questa schermata consente di creare e gestire i criteri IT da assegnare ai dispositivi BlackBerry attivi. I criteri controllano diversi fattori, quali la protezione mediante password o la crittografia dei file.

Domini 176: le opzioni di questa schermata consentono di scegliere il criterio predefinito da assegnare ai nuovi account di ogni dominio. Consentono inoltre di applicare un criterio agli account di dominio esistenti.

Account integrati 177: in questa schermata sono elencati tutti gli account BlackBerry attivati e il relativo stato, attivo o inattivo. Con gli account attivi viene indicato anche il PIN del dispositivo attivato. Inoltre, un pulsante nella parte inferiore della schermata consente di avviare una sincronizzazione lenta di tutti gli account attivi. In tal modo, vengono risincronizzati i dati di tutti gli account, a garanzia di coerenza tra i dati dei dispositivi e quelli di MDaemon.

Backup/Ripristino 178: questa schermata consente di effettuare il backup manuale del database BES e di specificare quanti file di backup notturni salvare.

Opzioni 180: questa schermata consente di impostare l'arresto dei servizi BES congiuntamente all'arresto di MDaemon, di configurare le opzioni di registrazione e di impostare numerose opzioni di sincronizzazione relative a messaggi di posta elettronica e dati di calendario.

Attivazione azienda

Per iniziare a utilizzare le funzionalità BES di MDaemon, è necessario che un account "attivi" un dispositivo BlackBerry con MDaemon. A questo scopo, effettuare la procedura descritta di seguito.

In MDaemon:

1. Passare a: Impostazioni » BlackBerry... » BES BlackBerry » Stato.
2. Fare clic su **Abilita BlackBerry Enterprise Server** se non è già selezionato.
3. Se si desidera creare un criterio personalizzato per il dispositivo, fare clic su **Criteri** 170 nel riquadro di sinistra.
4. Fare clic su **OK**.
5. Passare a: Account » Account Manager... e fare doppio clic sull'account per il quale si desidera consentire l'attivazione del dispositivo.
6. Fare clic su **BlackBerry BES** 350 nel riquadro di sinistra di Account Editor.
7. Fare clic su **Abilita questo account all'uso di BlackBerry**.
8. Scegliere un criterio nell'elenco a discesa.
9. Fare clic su **OK**.

Sul dispositivo dell'utente, procedere come indicato di seguito.

1. Disattivare o rimuovere eventuali client di sincronizzazione di terze parti, ad esempio il client SyncML, attualmente in uso per la sincronizzazione dei dati con l'account di MDaemon.
2. Se il dispositivo è configurato per ricevere i messaggi di posta elettronica dall'account mediante BIS (BlackBerry Internet Service), rimuovere l'account dalle impostazioni di configurazione dei messaggi di posta elettronica del dispositivo.
3. Se nel dispositivo sono presenti voci di calendario, è necessario eliminarle dal dispositivo o reimpostare il calendario. In caso contrario, non sarà possibile inviare al dispositivo i dati di calendario esistenti nel server MDaemon. Prima di questa operazione effettuare sempre il backup dei dati del dispositivo. **Nota:** se si sceglie di reimpostare il calendario, anziché eliminare i dati dal dispositivo, è possibile effettuare questa operazione successivamente all'attivazione. Per ulteriori informazioni, consultare **Reimpostazione del calendario del dispositivo** 182.

Nota: il mancato completamento dei precedenti Passaggi 1 e 2 può comportare la duplicazione dei messaggi di posta elettronica, delle voci di calendario o di altri dati PIM sul dispositivo.

In WorldClient è necessario eseguire quanto indicato di seguito.

1. Accedere a WorldClient.
2. Passare a: Opzioni » BlackBerry Management.
3. Connettere il dispositivo mediante un cavo USB e seguire le indicazioni visualizzate. È necessario disporre della versione 6 o di versioni successive di Internet Explorer.

   oppure

   Immettere la password di attivazione, fare clic su **Salva** e attivare il dispositivo via radio (OTA) direttamente dalla schermata Attivazione azienda del dispositivo. L'utente immetterà l'indirizzo di posta elettronica dell'account e la password di attivazione sul dispositivo. **Nota:** l'attivazione OTA non è disponibile per tutti i dispositivi.
4. Uscire da WorldClient.

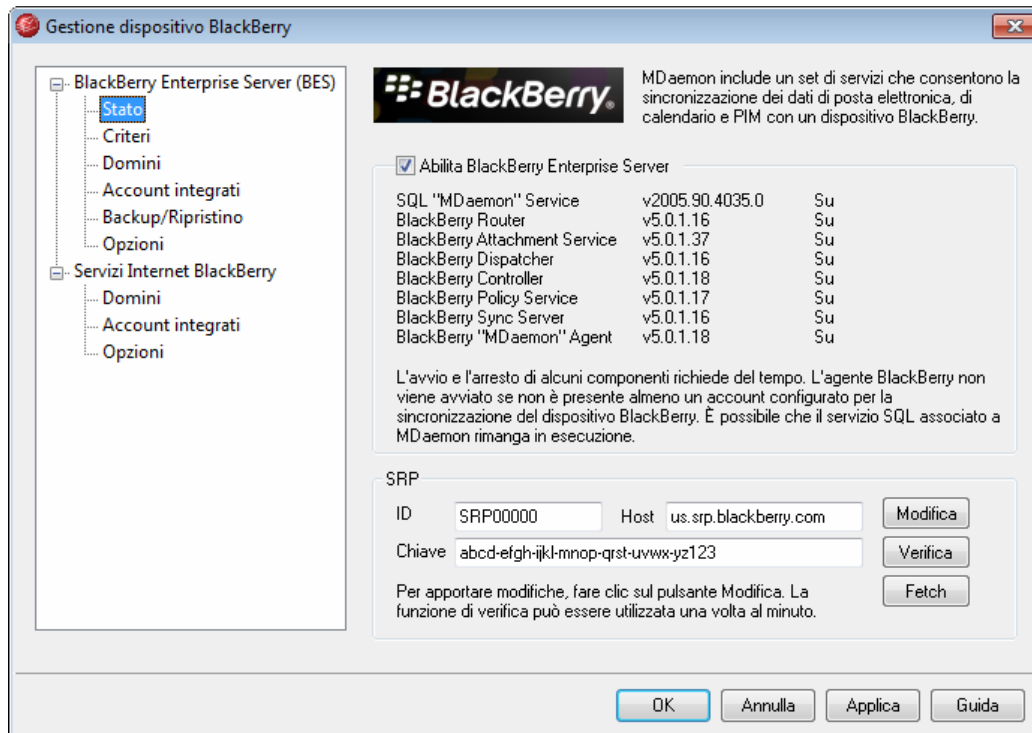
Dopo aver avviato il processo di attivazione, mediante cavo USB o OTA, questo proseguirà sul dispositivo fino al completamento. Al termine del processo, il dispositivo verrà associato all'account MDaemon/WorldClient. Dopo poco tempo, avrà inizio la sincronizzazione dei dati.

In base al dispositivo e al sistema operativo installato, l'attivazione potrebbe eliminare tutti i dati dal dispositivo, ripristinandone le impostazioni predefinite prima di sincronizzarlo con MDaemon/WorldClient. Per questo motivo, prima di attivare il dispositivo, è necessario che l'utente effettui un backup o esporti i dati che desidera conservare mediante Desktop Manager o altri programmi.

Dopo aver attivato un dispositivo, è possibile osservare diverse funzionalità modificate o differenze operative rispetto allo stato precedente ad Attivazione azienda. L'entità delle differenze dipende dal dispositivo, dal sistema operativo, dal criterio utilizzato e dall'eventuale precedente attivazione del dispositivo in un altro server BES.

Vedere:

Account Editor » BES BlackBerry 350
BIS BlackBerry 184

4.5.1.1 Stato

Questa schermata è disponibile in: Impostazioni » BlackBerry... » BES BlackBerry » Stato. Consente di abilitare o disabilitare il server BES, nonché di visualizzare lo stato dei diversi componenti e servizi. Vengono visualizzate anche le informazioni univoche sul protocollo SRP (Server Routing Protocol), inclusi l'ID e la chiave.

Abilita BlackBerry Enterprise Server

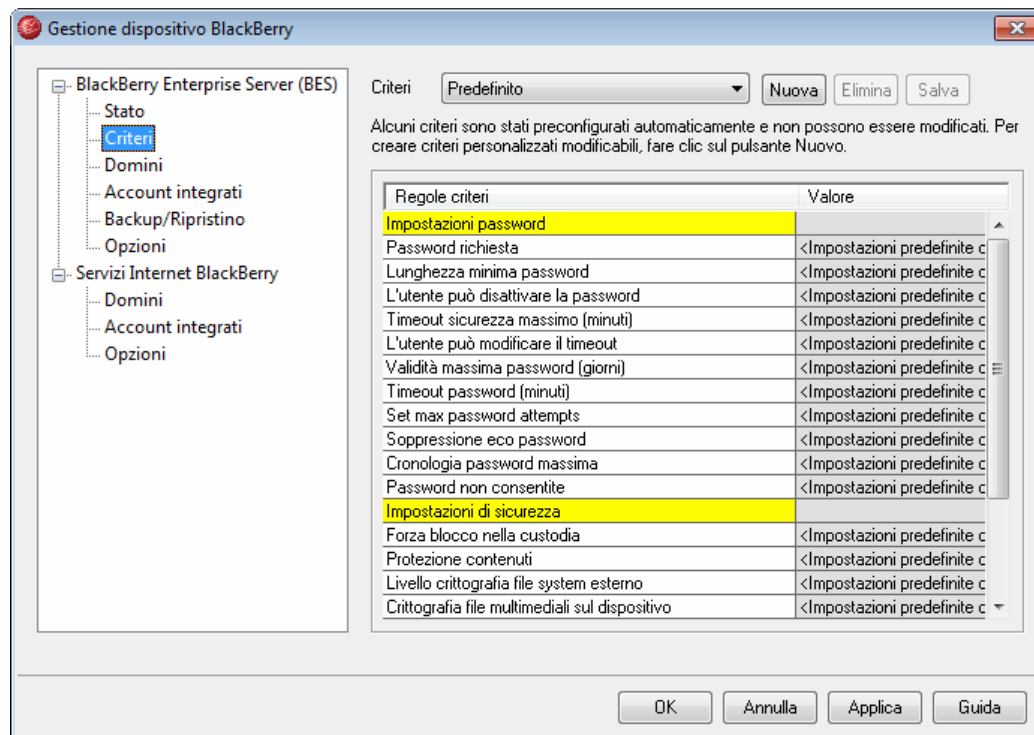
Questa casella consente di abilitare l'avvio dei diversi servizi BES (BlackBerry Enterprise Server). L'avvio o l'arresto completo di alcuni componenti può richiedere del tempo e il servizio "MDaemon" SQL potrebbe proseguire l'esecuzione durante l'arresto di BES. L'agente "MDaemon" di BlackBerry non viene avviato finché non sia stato abilitato per BlackBerry 350 almeno un account.

SRP

Il protocollo SRP (Server Routing Protocol) consente di autenticare e identificare il traffico tra MDaemon e i dispositivi BlackBerry sulle reti wireless. È necessario che MDaemon disponga di un ID SRP e di una chiave SRP univoci, ottenuti automaticamente durante l'installazione. Le credenziali SRP sono associate al server MDaemon e non possono essere utilizzate con altri server. Non dovrebbe essere necessario modificare queste informazioni, ma nel caso si verificasse tale esigenza è possibile servirsi del pulsante **Modifica**. Per confermare la validità delle credenziali SRP, fare clic su **Verifica**
.

Vedere:

[BES BlackBerry](165)
[Account Editor » BES BlackBerry](350)

4.5.1.2 Criteri

Quando si attiva un dispositivo BlackBerry in MDaemon, al dispositivo viene inviato un criterio specificato. I criteri sono serie di regole che indicano ciò che è necessario o consentito per un dispositivo. Le regole consentono di impostare le password, di bloccare il dispositivo quando è riposto nella custodia, di crittografare i file del dispositivo e altro ancora. È possibile assegnare i criteri ai domini e ai singoli account. Per assegnare i criteri ai domini utilizzare la schermata Domini[176] oppure, per assegnarli a determinati account, utilizzare la schermata BES BlackBerry[350] di Account Editor. In MDaemon sono disponibili tre criteri preconfigurati, ma è possibile crearne altri personalizzati.

Dopo aver attivato un dispositivo, è possibile osservare diverse funzionalità modificate o differenze operative rispetto allo stato precedente ad Attivazione azienda. L'entità delle differenze dipende dal dispositivo, dal sistema operativo, dal criterio utilizzato e dall'eventuale precedente attivazione del dispositivo in un altro server BES.

Criteri preconfigurati

Esistono tre criteri preconfigurati che non è possibile modificare o rimuovere:

Predefinito
Con questo criterio, il dispositivo BlackBerry utilizza i valori BES standard predefiniti per tutte le impostazioni. Si tratta di una configurazione dei criteri standard pronta all'uso relativa al controllo di un dispositivo BlackBerry mediante un server BES.

Password richiesta
Questo criterio è simile a *Predefinito*, fatta eccezione per l'impostazione della regola *Password richiesta* su `Sì` e della regola *L'utente può disattivare la password* su **No** (vedere le descrizioni successive delle regole). I dispositivi in cui viene impostato questo criterio devono essere protetti da password.

Scadenza password
Questo criterio è analogo a *Password richiesta*, ma determina anche l'impostazione della regola *Validità massima password (giorni)* su `30`. Con questo criterio è necessario modificare la password del dispositivo con una frequenza minima di 30 giorni.

Creazione di criteri personalizzati

Per creare un criterio personalizzato utilizzare la procedura seguente.

1. Fare clic su **Nuova**.
2. Immettere il nome del criterio.
3. Fare clic su **OK**.
4. Impostare le regole dei criteri come desiderato.
5. Fare clic su **Salva**.

Regole dei criteri

Viene riportato l'elenco di tutte le regole dei criteri che è possibile impostare quando si crea o si modifica un criterio personalizzato.

Impostazioni password

Contiene le regole dei criteri da applicare alle impostazioni delle password dei dispositivi BlackBerry.

Password richiesta
Specifica se per il dispositivo BlackBerry debba essere utilizzata una password. Se si imposta questa regola su **Sì**, è necessario che l'utente immetta la password per sbloccare il dispositivo BlackBerry.

Dipendenza tra regole: Se si attiva questa regola, è necessario impostare la regola *L'utente può disattivare la password* su **No** per impedire all'utente del dispositivo BlackBerry di disattivarla.

Lunghezza minima password
Digitare la lunghezza minima, in caratteri, desiderata per la password del dispositivo BlackBerry. Questa regola consente di controllare solo la lunghezza minima della password e non quella massima. La lunghezza massima consentita per la password è 32 caratteri. L'intervallo valido per i valori di questa regola è compreso tra 4 e 14.

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

L'utente può disattivare la password
Specifica se sia possibile disattivare la password obbligatoria sul dispositivo BlackBerry. Per impedire all'utente di disattivare la password obbligatoria sul dispositivo BlackBerry, impostare questa regola su **No**.

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

Timeout sicurezza massimo (minuti)
Specificare l'intervallo massimo, espresso in minuti, che l'utente può impostare sul dispositivo BlackBerry come valore del timeout di sicurezza, ossia il numero di minuti di inattività trascorso il quale è necessario digitare nuovamente la password per sbloccare il dispositivo. L'utente del dispositivo BlackBerry può impostare qualsiasi valore di timeout pari o inferiore al valore massimo, ammesso che il valore della regola *L'utente può modificare il timeout* non sia impostato su **No**. Il valore massimo del timeout di sicurezza disponibile per impostazione predefinita sul dispositivo BlackBerry è di 60 minuti. L'intervallo valido per i valori di questa regola è compreso tra **10 e 480** minuti.

Nota: per impostare uno specifico valore di timeout utilizzare la regola *Timeout password (minuti)*.

Dipendenza tra regole: il dispositivo BlackBerry può utilizzare questa regola del criterio solo se la regola *Password richiesta* è impostata su **Sì**.

L'utente può modificare il timeout
Indica se è possibile modificare il timeout di sicurezza del dispositivo BlackBerry. Se questa regola è impostata su **Sì**, l'utente può impostare il timeout su qualsiasi valore disponibile, purché compreso entro il limite impostato con la regola *Timeout sicurezza massimo (minuti)*. Per impedire all'utente di modificare il valore del timeout, impostare questa regola su **No**. In assenza di valori impostati, viene utilizzato il valore predefinito **Sì**.

Validità massima password (giorni)
Digitare il numero di giorni trascorso il quale scade la password del dispositivo BlackBerry e viene richiesto di impostare una nuova password. L'intervallo valido per i valori di questa regola è compreso tra **0 e 65535** giorni. **Nota:** per impedire la scadenza della password del dispositivo, impostare questa regola su **0**.

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

Timeout password (minuti)
Specificare la durata, espressa in minuti, dell'inattività dell'utente del dispositivo BlackBerry prima che scada il timeout di sicurezza, trascorso il quale è necessario digitare la password per sbloccare il dispositivo. L'intervallo valido per i valori di questa regola è compreso tra **0 e 60**.

Nota: l'intervallo del timeout di sicurezza predefinito è di 2 minuti di inattività per le versioni software dei dispositivi BlackBerry precedenti alla versione 4.7 e di 30 minuti di inattività per le versioni 4.7 e successive.

Dipendenze tra regole: il dispositivo BlackBerry può utilizzare questa regola solo se la regola *Password richiesta* è impostata su **Sì**. Se non si imposta la regola *L'utente può modificare il timeout* su **No**, l'utente del dispositivo BlackBerry può impostare il timeout della password su uno dei valori di un intervallo. Il valore massimo del timeout di sicurezza, disponibile per impostazione predefinita sul dispositivo BlackBerry, è di 60 minuti.

N. massimo tentativi password
Impostare il numero di tentativi di immissione della password consentiti per il dispositivo BlackBerry prima che i dati del dispositivo vengano cancellati e il dispositivo stesso venga disattivato. L'intervallo valido per i valori di questa regola è compreso tra **3 e 10** tentativi. Il valore predefinito è **10** tentativi consentiti.

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

Soppressione eco password
Impostando questa regola su **Sì** è possibile impedire la visualizzazione dei caratteri digitati nella schermata della password dopo che l'utente ha immesso il numero stabilito di password errate nel tentativo di sbloccare il dispositivo.

Nota: la regola *N. massimo tentativi password* consente di indicare il numero di password errate ammesso prima che i caratteri della password vengano visualizzati sullo schermo (se consentita).

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Perché venga richiesta la password, impostare la regola *Password richiesta* su **Sì**.

Cronologia password massima
Consente di impostare il numero massimo di password utilizzato dal dispositivo BlackBerry per verificare le nuove password al fine di evitare di riutilizzare quelle precedenti. L'intervallo valido per i valori di questa regola è compreso tra **0 e 15** password. Per impedire che il dispositivo verifichi le password riutilizzate, impostare questa regola su **0**. In assenza di impostazioni, viene

utilizzato il valore predefinito **0**.

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

Password non consentite
Digitare un elenco di valori di stringa separati da virgola che indichino le parole che non è possibile utilizzare nelle password.

Nota: il dispositivo BlackBerry impedisce automaticamente le sostituzioni delle lettere comuni. Se, ad esempio, si include nell'elenco delle parole vietate la parola "password", nel dispositivo non sarà possibile utilizzare "p@ssw0rd", "pa$zword" o "password123".

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

Impostazioni di sicurezza

Contiene le regole dei criteri da applicare per la sicurezza del dispositivo BlackBerry."

Forza blocchi nella custodia
Indicare se si desidera che nel dispositivo BlackBerry venga attivato il blocco di sicurezza quando viene riposto nella custodia. In assenza di impostazioni, viene utilizzato il valore predefinito **No**.

Protezione contenuti
Indicare se la protezione dei contenuti è attiva selezionando la robustezza dell'algoritmo crittografico utilizzato dal dispositivo BlackBerry per crittografare il contenuto ricevuto mentre è bloccato.

Quando la protezione dei contenuti è attiva, il contenuto del dispositivo BlackBerry è sempre protetto con l'algoritmo di crittografia AES a 256 bit. Un dispositivo BlackBerry, bloccato durante la ricezione del contenuto, genera in modo casuale la chiave di protezione dei contenuti (una chiave di crittografia AES a 256 bit) e una coppia di chiavi ECC, ricava una chiave di crittografia AES a 256 bit temporanea dalla password del dispositivo BlackBerry e la utilizza per crittografare la chiave di protezione del contenuto e la chiave privata ECC.

Dipendenza tra regole: il dispositivo BlackBerry può utilizzare questa regola del criterio solo se la regola *Password richiesta* è impostata su **Sì**.

Livello crittografia file system esterno
Specificare il livello di crittografia utilizzato dal dispositivo BlackBerry per crittografare i file archiviati in un file system esterno. Questa regola del criterio consente di richiedere al dispositivo BlackBerry la crittografia di un file system esterno, includendo o escludendo le directory multimediali. In assenza di impostazioni, viene utilizzato il valore predefinito **Livello 0** (ossia Non richiesto).

È possibile impostare questa regola sui seguenti valori:

Livello 0: Non richiesto

Livello 1: Crittografia con password utente (escluse directory multimediali)

Livello 2: Crittografia con password utente (incluse directory multimediali)

Livello 3: Crittografia con chiave dispositivo (escluse directory multimediali)

Livello 4: Crittografia con chiave dispositivo (incluse directory multimediali)

Livello 5: Crittografia con password utente e chiave dispositivo (escluse directory multimediali)

Livello 6: Crittografia con password utente e chiave dispositivo (incluse directory multimediali)

Crittografia file multimediali sul dispositivo
Specificare se i file multimediali situati nella memoria integrata del dispositivo, se disponibile, verranno crittografati con la password dell'utente e con la chiave generata dal dispositivo. Se si imposta questa regola su **Richiesta** o **Non consentita**, l'utente non può modificare l'impostazione sul dispositivo. In assenza di impostazioni, viene utilizzato il valore predefinito **Consentita**.

Dipendenza tra regole: il dispositivo BlackBerry utilizza questa regola del criterio solo se è impostata la regola *Protezione contenuti*.

Password richiesta per download applicazione
Specificare se il dispositivo BlackBerry richiederà all'utente la password prima di utilizzare il browser per scaricare le applicazioni.

Dipendenza tra regole: il dispositivo BlackBerry può servirsi di questa regola solo se è stata impostata una password. Per impostare una password sul dispositivo BlackBerry, impostare la regola *Password richiesta* su **Sì**.

Disabilita l'accesso ai dati dell'organizer per le applicazioni di social networking
Questa regola specifica se il dispositivo BlackBerry impedirà alle applicazioni di social networking di accedere a dati quali i contatti e i dati di calendario. Per consentire alle applicazioni di social networking l'accesso alla rubrica, al calendario e agli altri dati, impostare la regola su **No**. Il valore predefinito di questa regola è **Sì**: le applicazioni di social networking non possono accedere ai dati del dispositivo.

Altro

Impostazioni varie

Consenti caricamento software basato su Web
Indica se consentire all'utente di aggiornare il software del dispositivo BlackBerry grazie alla funzione di caricamento software basata sul Web. In

assenza di impostazioni, viene utilizzato il valore predefinito **No**.

Nome autore criterio
Immettere il nome dell'autore del criterio.

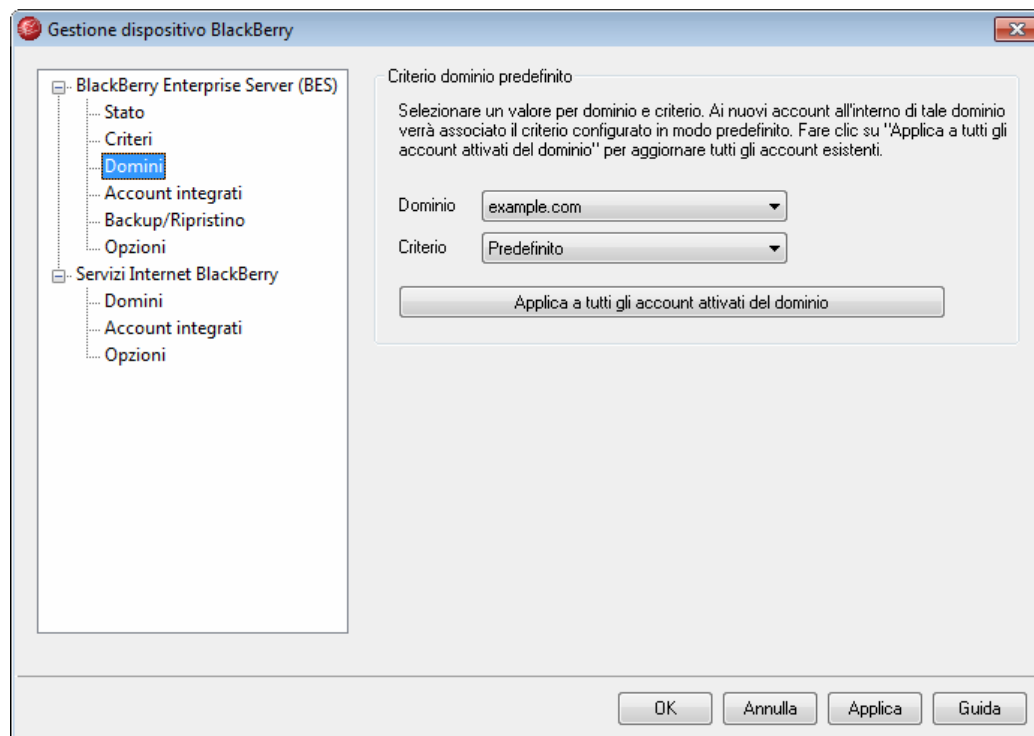
Descrizione criterio
Inserire un breve testo descrittivo del criterio.

Vedere:

BES BlackBerry 165

Domini 176

Account Editor » BES BlackBerry 350

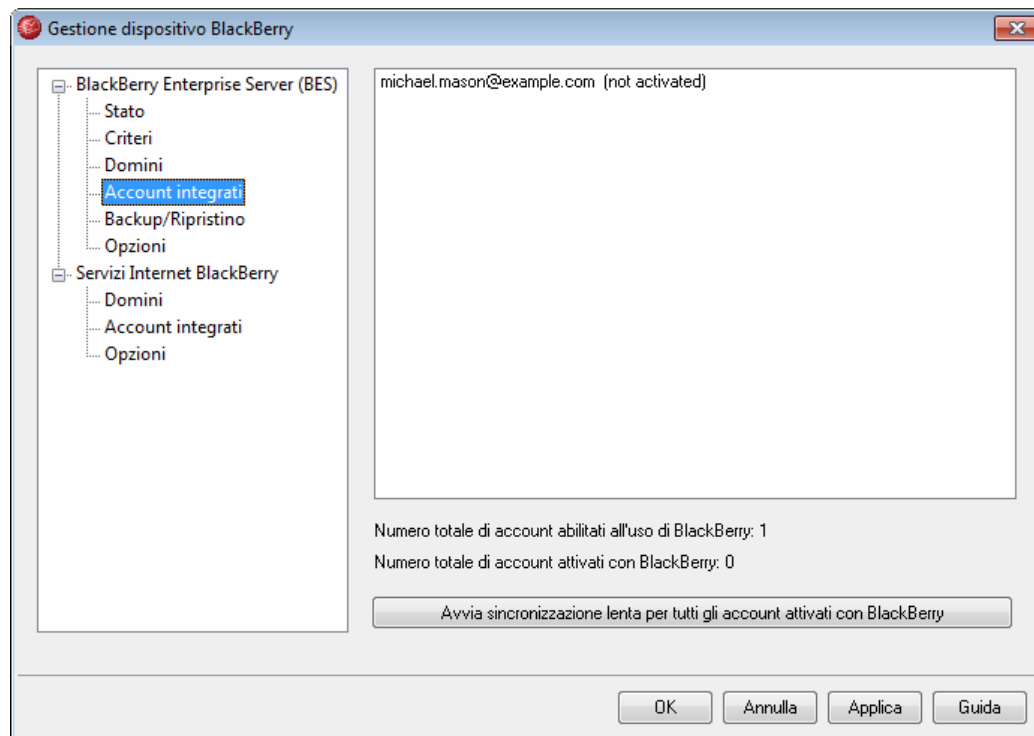
4.5.1.3 Domini

Criterio dominio predefinito
Per indicare il criterio 170 predefinito da assegnare a ogni nuova attivazione BlackBerry in un determinato dominio, selezionare il dominio desiderato nell'elenco a discesa, selezionare il criterio da assegnare a tutte le nuove attivazioni e fare clic su **OK**. Questo criterio verrà assegnato solo alle nuove attivazioni. Le attivazioni esistenti non verranno modificate.

Applica a tutti gli account attivati del dominio

Per applicare un criterio a tutti i dispositivi di un dominio già attivati, selezionare un dominio e un criterio negli elenchi a discesa e fare clic su questo pulsante. Il criterio verrà applicato a **tutti** gli account di dominio attivati, anche a quelli cui è già stato assegnato un diverso criterio nella schermata BES BlackBerry 350 di Account Editor.

Vedere:

BES BlackBerry 165
Account Editor » BES BlackBerry 350

4.5.1.4 Account integrati

In questa schermata sono elencati tutti gli account BlackBerry attivati e il relativo stato: attivo o inattivo. Con gli account attivi viene indicato anche il PIN del dispositivo attivato. Nell'elenco degli account è presente un contatore che indica il numero degli account abilitati per BlackBerry e di quelli attivati.

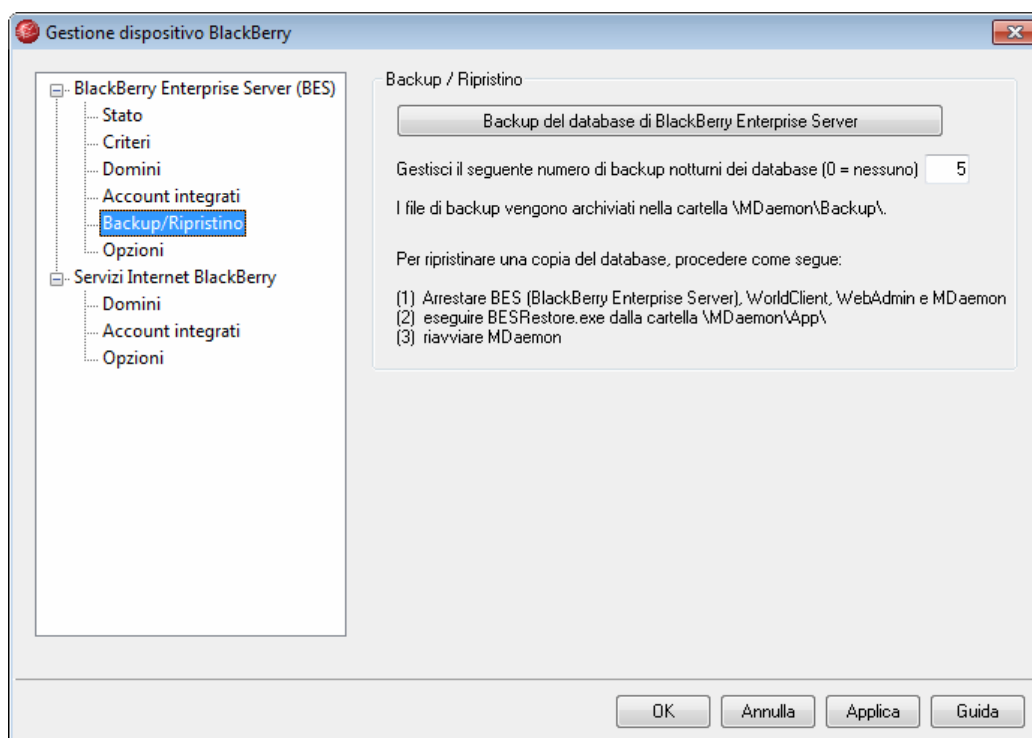
Avvia sincronizzazione lenta per tutti gli account attivati con BlackBerry

Questo pulsante consente di avviare un'operazione di sincronizzazione lenta per tutti gli account attivati. In tal modo i dati di tutti gli account vengono risincronizzati per garantire la coerenza tra i dati dei dispositivi e quelli di MDaemon. In base al numero degli account e all'entità dei dati da sincronizzare, il completamento di questa operazione potrebbe richiedere del tempo. Dopo l'avvio, l'operazione viene eseguita in background fino al completamento. Verrà richiesto di confermare l'avvio

dell'operazione di sincronizzazione lenta. Un'opzione della schermata BES BlackBerry 350 di Account Editor consente di avviare l'operazione di sincronizzazione lenta per uno specifico account. Per ulteriori informazioni sulle opzioni di sincronizzazione BES, consultare Opzioni 180.

Vedere:

BES BlackBerry 165
Account Editor » BES BlackBerry 350
BES BlackBerry » Opzioni 180

4.5.1.5 Backup/Ripristino

Backup del database BES

Le opzioni della schermata Backup/Ripristino consentono di ottenere un backup del database BES.

Backup dei file di database BES
Questo pulsante consente di ottenere un backup manuale immediato del database BES. Il file di backup viene memorizzato nella cartella `\MDaemon\Backup\`. Nella scheda Sistema della schermata principale di MDaemon 30 viene visualizzata una riga relativa all'avanzamento del processo di backup.

Gestisci il seguente numero di backup notturni dei file di database BES (0 = nessuno)
Ogni notte viene eseguita una copia di backup del database BES e i relativi file

vengono memorizzati nella cartella `\MDaemon\Backup\`. Questa opzione determina il numero di file di backup da salvare. Raggiunto il limite, quando viene creato un nuovo file di backup quello meno recente viene cancellato. Il valore "0" indica che non si desidera eseguire backup notturni automatici.

Questo valore limita il numero dei file di backup salvati e include i backup manuali avviati mediante il pulsante *Backup dei file di database BES*. Se tale valore viene impostato su "0", non vengono eseguiti backup notturni, ma è comunque possibile eseguire backup manuali e il numero di file salvati è illimitato.

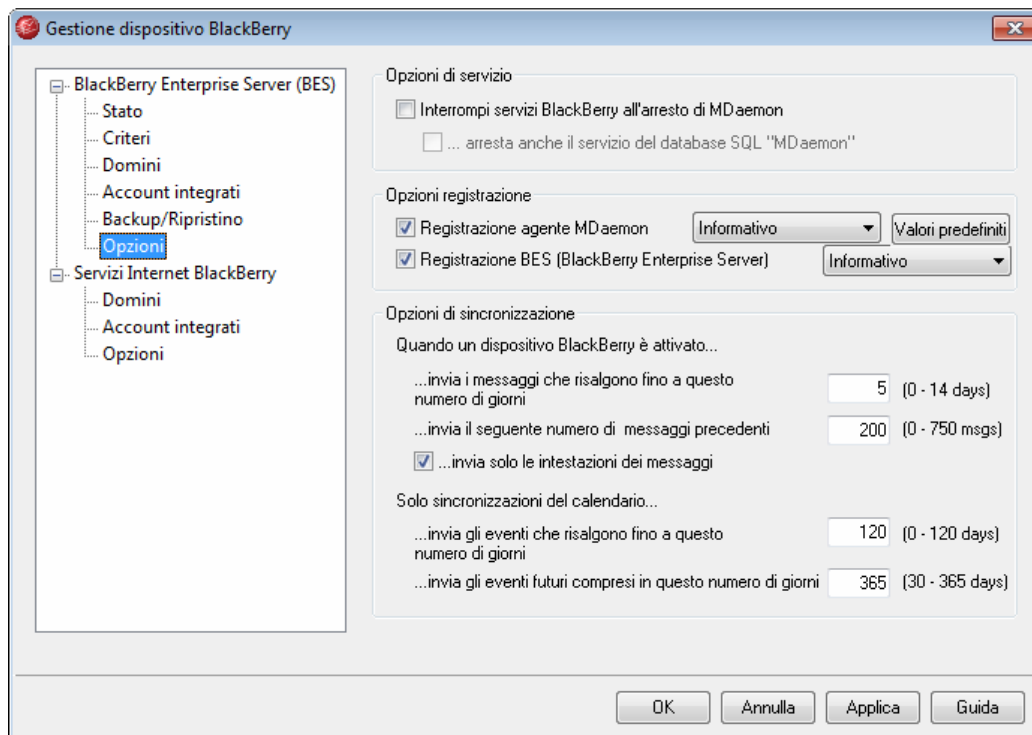
Ripristino del database BES

Per ripristinare il database BES da un file di backup:

1. Arrestare BES, WorldClient, WebAdmin e, infine, MDaemon.
2. Eseguire l'utilità di ripristino del database BES di MDaemon (`BESRestore.exe`) situata nella cartella `\MDaemon\App\`.
3. Fare clic su **Browse** e selezionare il file di backup.
4. Fare clic su **Open**.
5. Fare clic su **Restore Now**.
6. Riavviare MDaemon, WebAdmin, WorldClient e BES.

Vedere:

BES BlackBerry 165
Account Editor » BES BlackBerry 350

4.5.1.6 Opzioni

Questa schermata consente di impostare l'arresto dei servizi BES insieme all'arresto di MDaemon, di configurare le opzioni di registrazione e di impostare numerose opzioni di sincronizzazione relative ai messaggi di posta elettronica e ai dati di calendario.

Opzioni di servizio

Interrompi servizi BlackBerry all'arresto di MDaemon
Selezionare questa casella di controllo per arrestare i servizi BlackBerry 169 insieme a MDaemon.

...arresta anche il servizio del database SQL "MDaemon"
Se si configura l'arresto dei servizi BlackBerry insieme a MDaemon e si desidera arrestare anche il servizio di database SQL "MDaemon", selezionare questa casella di controllo. Il servizio di database "MDaemon" SQL viene, generalmente, lasciato in esecuzione, anche quando si arresta MDaemon o i servizi BlackBerry.

Opzioni registrazione

Sono disponibili due opzioni di registrazione: **Registrazione agente MDaemon** e **Registrazione componente BES**. È possibile attivarle o disattivarle separatamente e impostare il livello di dettaglio della registrazione di ciascuna di esse. È possibile scegliere tra quattro livelli di dettaglio della registrazione: *Errore*, *Avviso*, *Informativo* e *Debug*. *Errore* è il livello di dettaglio della registrazione più basso, mentre *Debug* è il più elevato e viene utilizzato, in genere, solo per la diagnosi dei problemi. *Informativo* consente di ottenere un buon livello di dettaglio ed è l'impostazione predefinita per entrambe le opzioni. **Valori predefiniti** consente di ripristinare i livelli di registrazione sulle impostazioni predefinite.

I servizi BES vengono riavviati ogni volta che si modifica il livello di registrazione.

I file di registro BlackBerry utilizzano le impostazioni di registrazione 108 globali di MDaemon per quanto riguarda la dimensione e la creazione, ma il formato è leggermente diverso da quello degli altri registri di MDaemon. I registri vengono memorizzati nella sottocartella `\Logs\BES\`.

Opzioni di sincronizzazione

Quando un dispositivo è attivato...
Grazie a questa opzione, quando un dispositivo BlackBerry viene attivato per la prima volta, viene sincronizzata non solo la nuova posta, ma anche parte della posta precedente, ossia quella inviata o ricevuta prima dell'attivazione. Viene sincronizzata con il dispositivo tutta la posta elaborata per l'account tra il momento di abilitazione BlackBerry 350 e quello di attivazione del dispositivo. Se il numero dei messaggi specificato direttamente o indirettamente (in base al numero di giorni) è inferiore al numero di messaggi associati alla sincronizzazione iniziale, in base alle opzioni verranno sincronizzati ulteriori messaggi.

...invia al BlackBerry i messaggi che risalgono fino a questo numero di giorni
Questa opzione consente di impostare il numero minimo di giorni in base al quale inviare i messaggi precedenti al dispositivo quando viene attivato. Se è impostata su 5, ad esempio, al dispositivo vengono inviati, come minimo, i messaggi degli ultimi cinque giorni.

Questa impostazione viene utilizzata anche durante la risincronizzazione (sincronizzazione lenta 177). La sincronizzazione lenta aggiunge i messaggi mancanti dal database solo se rientrano nel numero di giorni specificato in questa opzione.

...invia al BlackBerry solo questo numero di messaggi precedenti
Questa opzione consente di impostare il numero di messaggi precedenti da sincronizzare con il dispositivo alla prima attivazione. Questa opzione ha la precedenza sull'opzione "*...invia al BlackBerry i messaggi che risalgono fino a questo numero di giorni*" già descritta. Il numero di messaggi elaborato dalla sincronizzazione iniziale, successiva all'attivazione, può superare il numero qui indicato se il numero di messaggi elaborati tra il momento dell'attivazione dell'account BlackBerry e quello dell'attivazione del dispositivo è superiore. Per impostazione predefinita, questa opzione è impostata su **200.**

...invia solo le intestazioni dei messaggi
Questa opzione consente di inviare al dispositivo, durante la sincronizzazione dei messaggi precedenti, solo l'intestazione e non l'intero messaggio.

Solo sincronizzazioni del calendario...
Queste opzioni determinano il numero di eventi di calendario da sincronizzare con i

dispositivi BlackBerry attivati. Quando si modificano tali valori, è necessario effettuare un'operazione di sincronizzazione lenta 177 in modo che gli eventi interessati dalle modifiche possano essere aggiunti o eliminati dai dispositivi. Un'operazione di sincronizzazione lenta del calendario si verifica automaticamente ogni notte a mezzanotte.

...invia al BlackBerry gli eventi che risalgono fino a questo numero di giorni
Numero di giorni degli eventi di calendario trascorsi interessati dalla sincronizzazione del calendario del dispositivo BlackBerry. Gli eventi ricorrenti, trascorsi da un numero di giorni superiore a quello indicato, vengono comunque visualizzati nel calendario del dispositivo se una delle occorrenze rientra nell'intervallo indicato.

...invia al BlackBerry gli eventi per questo numero di giorni futuri
Numero di giorni degli eventi di calendario futuri interessati dalla sincronizzazione con il dispositivo BlackBerry.

Se, prima dell'attivazione, nel dispositivo sono presenti voci di calendario, è necessario cancellare tutti i dati del dispositivo o reimpostare il calendario. In caso contrario, non sarà possibile inviare al dispositivo i dati di calendario esistenti nel server MDaemon. Se si sceglie di reimpostare il calendario, anziché eliminare i dati dal dispositivo, è possibile effettuare questa operazione successivamente all'attivazione. Per ulteriori informazioni, consultare **Reimpostazione del calendario del dispositivo** più avanti. Effettuare sempre il backup dei dati del dispositivo prima di cancellarli o di reimpostare il calendario.

⊟ Reimpostazione del calendario del dispositivo

Panoramica (articolo KB15139)

Attenzione: le seguenti procedure consentono di eliminare tutti i dati di calendario dallo smartphone BlackBerry e di risincronizzare nuovamente il calendario con lo smartphone.

Nota: effettuare il backup dei dati prima di eseguire la procedura. Per istruzioni, consultare l'articolo KB12487.

Completare la procedura relativa alla versione software del dispositivo BlackBerry installata nello smartphone.

Dispositivo BlackBerry con versione software 4.2

Sullo smartphone BlackBerry, effettuare la seguente procedura:

1. Nel menu dell'applicazione Calendario, fare clic su **Opzioni**.
2. Scorrere la schermata e, in fondo, digitare **RSET**.

Nota: per gli smartphone BlackBerry dotati di tecnologia SureType®, utilizzare il metodo di input a tocco multiplo.

Dispositivo BlackBerry con versioni software da 4.3 a 5.0

Sullo smartphone BlackBerry, effettuare la seguente procedura:

1. Nel menu dell'applicazione Calendario, fare clic su **Opzioni**.
2. Nella schermata Opzioni, digitare **RSET**.

Nota: per gli smartphone BlackBerry dotati di tecnologia SureType, utilizzare il metodo di input a tocco multiplo.

Informazioni aggiuntive

Processo di sincronizzazione di calendario wireless

Sincronizzazione di calendario wireless attiva

Se la sincronizzazione di calendario wireless è **attiva**, viene visualizzato il seguente messaggio:

> *This will erase your <nameofcalendar> calendar, and reload it from your server. Continue? (Il calendario <NomeCalendario> verrà cancellato e ricaricato dal server. Continuare?*

Dopo aver eliminato i dati di calendario, viene visualizzato il seguente messaggio:

> *The <nameofcalendar> calendar has been wiped. It will be repopulated from your server (Il calendario <NomeCalendario> è stato cancellato e verrà ricaricato con i dati del server).*

Il calendario viene ricaricato con i dati di calendario del server BES.

Sincronizzazione di calendario wireless inattiva

Se la sincronizzazione di calendario wireless è **inattiva**, viene visualizzato il seguente messaggio:

> *Wireless Calendar, for <nameofcalendar>, is not enabled. Wipe Calendar anyway (Il calendario wireless per <NomeCalendario> non è abilitato. Cancellare i dati del calendario)?*

Dopo aver eliminato i dati di calendario, viene visualizzato il seguente messaggio:

> *The <nameofcalendar> calendar has been wiped (I dati del calendario <NomeCalendario> sono stati cancellati).*

È necessario, quindi, ricaricare il calendario con i dati utilizzando BlackBerry Desktop Manager e la sincronizzazione via cavo.

Ricaricamento del calendario

Durante il ricaricamento del calendario, nello smartphone BlackBerry può essere visualizzato il seguente messaggio:

Organizing Calendar (Organizzazione calendario in corso)

Il ricaricamento del calendario può influire sulle prestazioni dello smartphone BlackBerry. La velocità di caricamento dipende dalla quantità di dati trasmessi e dalla velocità della rete wireless.

Vedere:

BES BlackBerry 165
Account Editor » BES BlackBerry 350

4.5.2 BIS BlackBerry

MDaemon include il supporto diretto per i servizi Internet BlackBerry (BIS, BlackBerry Internet Service). Gli utenti BIS possono integrare l'account di posta di MDaemon con il proprio smartphone BlackBerry, inviare la posta tramite BlackBerry e gestire la posta con funzioni avanzate utilizzando un dispositivo BlackBerry e MDaemon. I dispositivi BlackBerry configurati per ricevere la posta da MDaemon tramite IMAP o POP nelle versioni di MDaemon precedenti alla 11.0 possono ora essere impostati per inviarla. I messaggi composti sul dispositivo, inoltre, vengono inviati a MDaemon per la consegna, senza utilizzare i server BIS. In tal modo, i messaggi di posta elettronica composti con un dispositivo BlackBerry saranno conformi ai criteri di protezione, alle regole di filtro dei contenuti, alla tecnologia DKIM, ai criteri di archiviazione e alle altre configurazioni implementate nel server dell'organizzazione.

Poiché i servizi BIS consentono di raccogliere la posta solo dalla casella Posta in arrivo degli utenti, si potrebbero verificare problemi se si utilizzano filtri IMAP 353 per ordinare automaticamente i messaggi in cartelle specifiche. Per risolvere il problema, la schermata Posta in arrivo BlackBerry 352 di Account Editor e la pagina Cartelle di WorldClient consentono, rispettivamente, agli amministratori e agli utenti di selezionare le cartelle che contengono i nuovi messaggi da recapitare al dispositivo. Quando il server BIS si connette a MDaemon per raccogliere i nuovi messaggi dalla Posta in arrivo dell'utente, MDaemon invia anche i nuovi messaggi delle cartelle selezionate. Tutti i nuovi messaggi delle cartelle selezionate vengono inviati alla Posta in arrivo del dispositivo BlackBerry. In tal modo, al dispositivo non vengono inviate le cartelle intere, ma solo i nuovi messaggi.

Infine, uno schema di gestione degli alias delle cartelle interne consente di assegnare alle cartelle "Posta inviata" e "Posta eliminata" di ogni utente valori riconosciuti da BIS, indipendentemente dal nome assegnato alle cartelle nell'account dell'utente. Ciò consente di collocare la posta inviata ed eliminata nelle cartelle di MDaemon appropriate.

La sezione BIS BlackBerry della finestra di dialogo BlackBerry include le seguenti

schermate:

Domini 186: consente di attivare l'integrazione BIS per i domini desiderati. Le opzioni disponibili consentono di immettere l'URL di iscrizione e il server SMTP ai quali BIS trasmetterà i messaggi creati con il dispositivo BlackBerry. Nella parte inferiore della schermata, è presente la casella di testo della cronologia in cui sono elencate tutte le attività di iscrizione o ritiro BIS, nonché numerose opzioni relative ai protocolli SSL e STARTTLS.

Account integrati 188: in questa schermata sono elencati i numeri di iscrizione di tutti gli account di MDaemon impostati per l'invio di posta BIS e, pertanto, direttamente integrati con MDaemon. Il server BIS può raccogliere la posta per conto del dispositivo BlackBerry mediante POP3 o IMAP anche per gli account non elencati tra quelli integrati, ma senza il vantaggio di poter inviare messaggi tramite il server MDaemon.

Opzioni 190: questa schermata comprende numerose impostazioni globali che governano le funzioni di integrazione di BlackBerry MDaemon. Le opzioni disponibili consentono, ad esempio, di inviare la posta dalle cartelle diverse da Posta in arrivo di MDaemon, di applicare la funzione Collegamento allegati 154 agli account integrati, di integrare più dispositivi con un singolo account di MDaemon e di utilizzare numerose altre caratteristiche.

Per l'accesso a MDaemon è necessario che tutte le sessioni IMAP/POP degli utenti BIS utilizzino un indirizzo di posta elettronica completo. Di conseguenza, quando si configurano i dispositivi BlackBerry per la raccolta di posta, è necessario utilizzare come parametro di accesso l'indirizzo di posta elettronica completo, anziché la sola porzione di indirizzo relativa alla casella postale. Questa operazione è necessaria per evitare possibili conflitti e garantire la corretta integrazione degli account. Per alcuni utenti può essere necessario eliminare e ricreare nuovamente il profilo di posta sul proprio dispositivo o, perlomeno, modificare il valore di accesso con l'indirizzo completo.

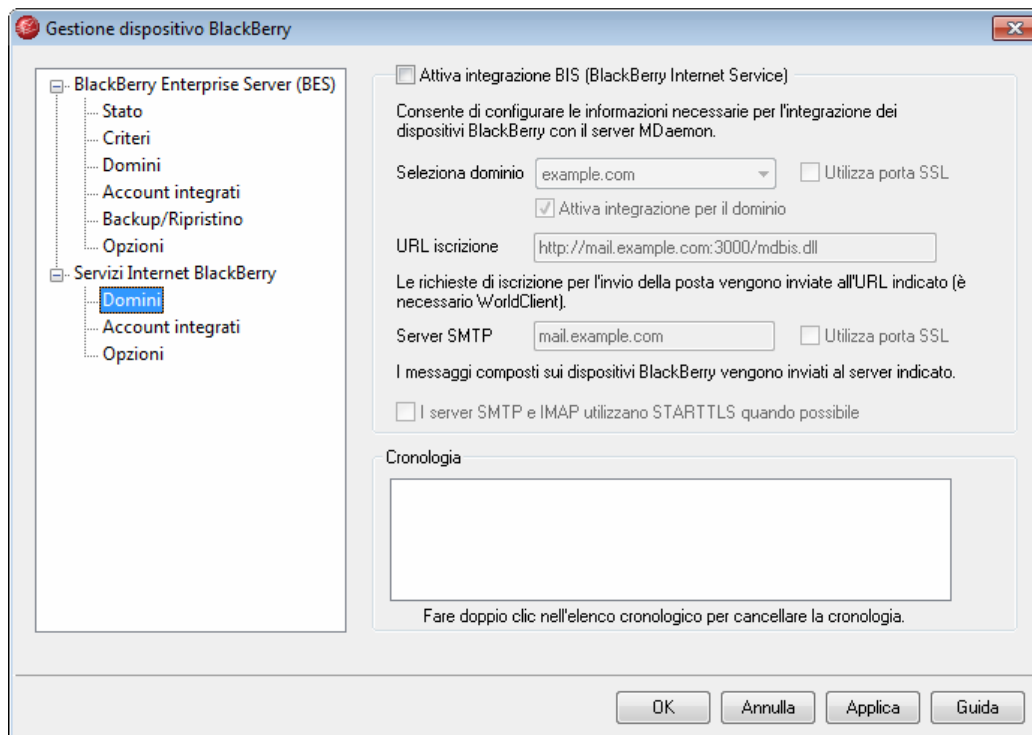
Vedere:

BIS BlackBerry » Domini 186

BIS BlackBerry » Account integrati 188

BIS BlackBerry » Opzioni 190

Account Editor » BIS BlackBerry 352

4.5.2.1 Domini

Attiva integrazione BIS (BlackBerry Internet Service)

Questa casella di controllo consente di attivare la funzione di integrazione BIS di MDaemon. Le opzioni seguenti consentono di attivarla/disattivarla per i singoli domini.

Quando l'integrazione BIS viene disattivata a livello globale o per determinati domini, gli account già iscritti a BIS continuano a operare come di consueto. Non verranno integrati ulteriori dispositivi BlackBerry, ma le integrazioni esistenti rimarranno invariate.

Seleziona dominio

Selezionare nell'elenco a discesa il dominio da configurare per l'integrazione BIS. Le modifiche apportate alle altre impostazioni si applicheranno solo a quel dominio.

Abilita integrazione BIS per il dominio

Questa opzione consente di attivare la funzione di integrazione BIS per il dominio selezionato.

Utilizza porta SSL

Se si è abilitato SSL[312] in MDaemon, con questa casella di controllo il client IMAP BIS utilizzerà la porta SSL dedicata. Il client IMAP BIS supporta il protocollo SSL solo sulla porta dedicata.

URL iscrizione

URL di WorldClient al quale il server BIS invia le richieste di iscrizione e ritiro. Quando si aggiunge un account di posta elettronica MDaemon a un dispositivo BlackBerry, BIS invia una richiesta di iscrizione all'URL entro venti minuti circa. MDaemon quindi aggiunge l'account alla schermata Account integrati 188. Le richieste di iscrizione sono gestite da WorldClient che, quindi, deve essere in funzione.

Quando si utilizza IIS invece del server Web nativo di WorldClient, è necessario aggiungere `MDbis.dll` (situato in `MDaemon\Worldclient\HTML\`) a IIS affinché i comandi SUBSCRIBE in entrata vengano elaborati correttamente.

Server SMTP

Server SMTP al quale vengono inviati per la consegna tutti i messaggi di posta elettronica creati mediante il dispositivo integrato con l'account.

Utilizza porta SSL

Se si è abilitato SSL 312 in MDaemon, selezionando questa casella di controllo il client SMTP BIS utilizzerà la porta SSL dedicata.

Il client SMTP BIS non supporta SSL con certificati autofirmati. Pertanto, per utilizzare SSL, è necessario utilizzare un certificato di terze parti reperibile in commercio.

I server SMTP e IMAP usano STARTTLS quando possibile

Se si è abilitata la funzione STARTTLS 312 di MDaemon, selezionando questa casella di controllo i server SMTP e IMAP utilizzano STARTTLS ogniqualvolta sia possibile.

BIS non supporta STARTTLS con certificati autofirmati. Pertanto, per utilizzare STARTTLS, è necessario utilizzare un certificato di terze parti reperibile in commercio.

Cronologia

In questa casella è elencata la cronologia di iscrizione/ritiro BIS degli account dell'utente. Per ogni voce è indicato se si tratta di un'azione di iscrizione o di ritiro, l'indirizzo di posta elettronica, nonché la data e l'ora dell'attività.

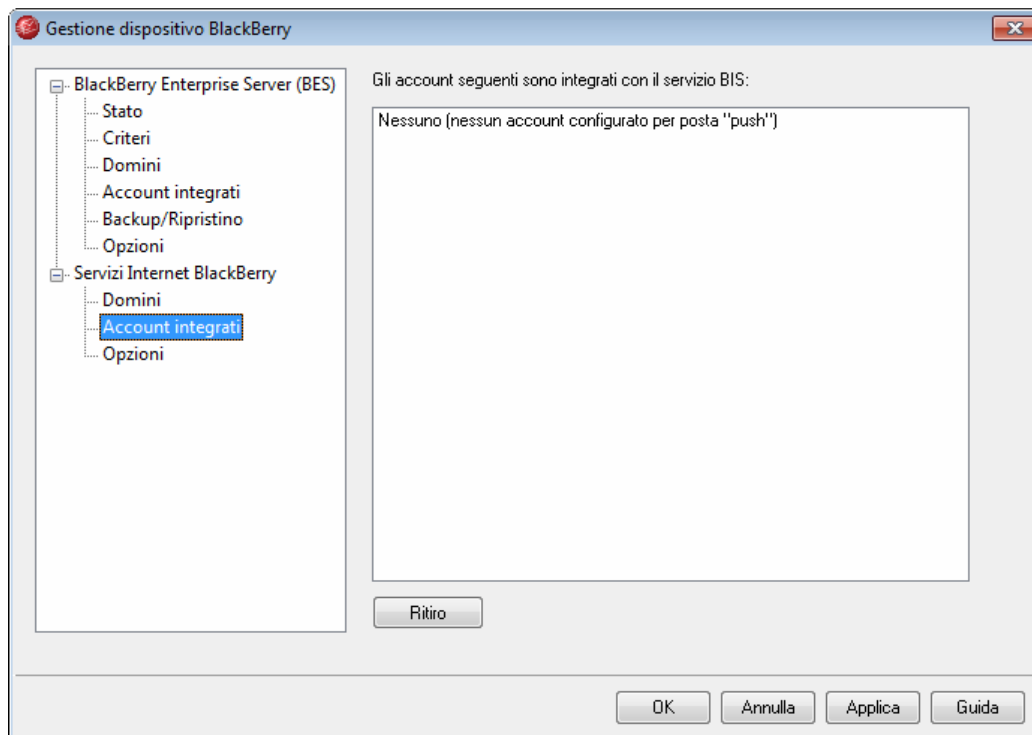
Vedere:

BIS BlackBerry 184

BIS BlackBerry » Account integrati 188

BIS BlackBerry » Opzioni 190

Account Editor » BIS BlackBerry 352

4.5.2.2 Account integrati

Configurazione degli account per l'invio di posta a uno smartphone BlackBerry

Nella schermata Account integrati sono elencati tutti gli account di MDaemon configurati per l'invio della posta a uno smartphone BlackBerry. Per impostare un nuovo account per l'invio di posta, procedere come indicato di seguito.

1. Abilitare le opzioni di integrazione BIS per il server e il dominio nella schermata Domini 186 e assicurarsi che i valori di *URL iscrizione* e *Server SMTP* facciano riferimento rispettivamente a WorldClient e al server MDaemon.
2. Se lo smartphone BlackBerry già raccoglie la posta dall'account MDaemon dell'utente, poiché l'account è stato aggiunto al dispositivo prima di attivare le funzioni BIS di MDaemon, eliminare l'account di posta elettronica dal dispositivo. Nel passaggio successivo, è necessario creare nuovamente l'account nel dispositivo in modo da poter configurare l'invio della posta con BIS.
3. Aggiungere l'account di posta elettronica di MDaemon allo smartphone BlackBerry utilizzando, come credenziali di accesso, l'**indirizzo di posta elettronica completo** e la password. Per istruzioni dettagliate sull'aggiunta di un account di posta elettronica a uno smartphone BlackBerry, consultare la Guida in linea o la documentazione del dispositivo. È necessario solo aggiungere l'account, senza modificarlo. Dopo aver creato l'account, non modificarne la firma, le impostazioni relative al nome, le opzioni avanzate o altre caratteristiche. Le modifiche potranno essere apportate successivamente, con il passaggio 6.

4. Poco dopo aver aggiunto l'account al dispositivo, l'*URL di iscrizione* associato con il dominio dell'utente riceverà una richiesta SUBSCRIBE dal servizio BIS. La richiesta in arrivo viene elaborata da WorldClient e l'account iscritto viene visualizzato nell'elenco degli account integrati. La richiesta SUBSCRIBE generalmente arriva in 5 minuti, ma può impiegarne anche 20.

5. Quasi subito dopo aver aggiunto l'account al dispositivo, si riceve il messaggio di posta elettronica "*Email activation information*" (Avviso di attivazione della posta elettronica). Quindi, dopo la ricezione e la corretta elaborazione della richiesta SUBSCRIBE, il dispositivo BlackBerry riceve un secondo messaggio di posta elettronica: "*Email activation information (push mail)*" (Avviso di attivazione della posta elettronica: invio posta). Dopo il secondo messaggio di posta elettronica, l'account è correttamente configurato per l'invio della posta con MDaemon.

6. È ora possibile apportare tutte le modifiche desiderate all'account di posta elettronica sul dispositivo. È possibile aggiungere una firma, modificare il nome, specificare le impostazioni avanzate e così via.

In attesa dell'arrivo della richiesta SUBSCRIBE da BIS, qualsiasi modifica apportata all'account di posta elettronica del dispositivo, ad esempio il testo della firma, le opzioni di configurazione avanzate e così via, invaliderebbe la richiesta impedendo la ricezione del messaggio. È pertanto necessario evitare di apportare modifiche all'account del dispositivo fino all'arrivo della richiesta SUBSCRIBE. In caso contrario, per riavviare il processo SUBSCRIBE sarà necessario eliminare l'account e crearne uno nuovo.

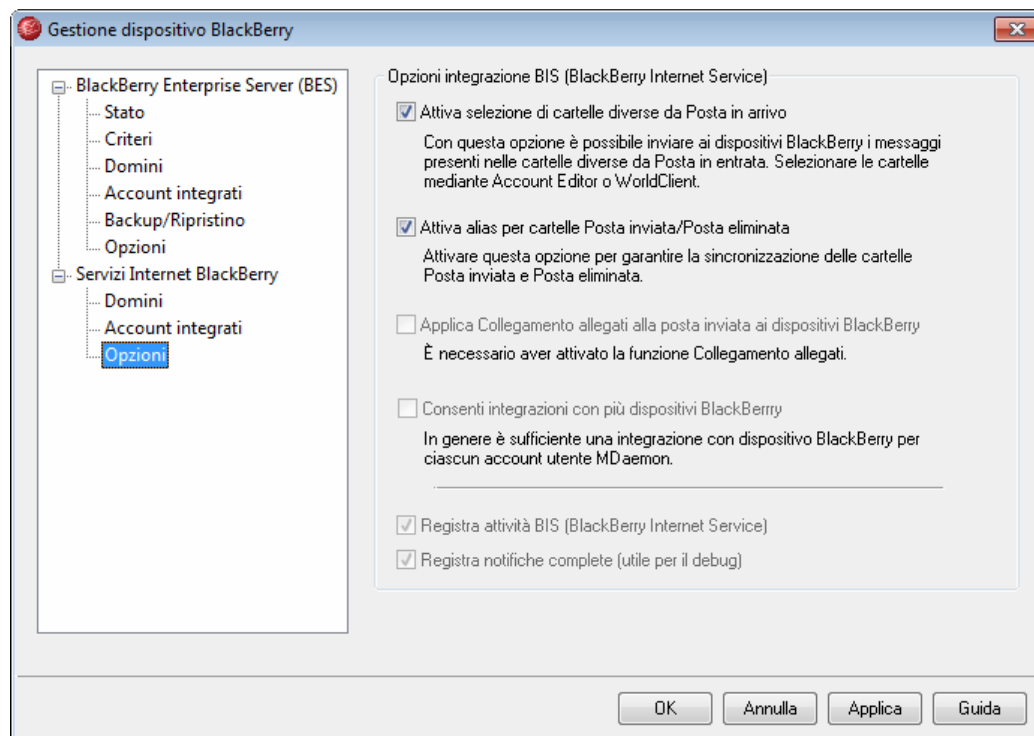
Questo livello di integrazione non è consentito con il protocollo POP. Gli utenti BlackBerry che raccolgono la posta utilizzando POP, dovranno eliminare il profilo di posta elettronica e crearne uno nuovo utilizzando IMAP (non POP), operazione che potrebbe richiedere l'accesso alle opzioni di configurazione avanzate di BlackBerry. Di conseguenza, per questa funzione è necessario che il server IMAP di MDaemon sia in esecuzione.

Ritiro di un account integrato

È possibile ritirarsi dall'invio della posta eliminando il profilo di posta elettronica con il dispositivo BlackBerry stesso. BIS invierà a MDaemon una richiesta UNSUBSCRIBE e il collegamento dell'account viene annullato. L'arrivo della richiesta UNSUBSCRIBE potrebbe richiedere del tempo, ma ciò non comporta problemi operativi.

See:

BlackBerry BIS 184
BlackBerry BIS » Domains 186
BlackBerry BIS » Options 190
Account Editor » BlackBerry BIS 352

4.5.2.3 Opzioni

Opzioni integrazione BIS

Queste opzioni consentono di selezionare il contenuto delle cartelle diverse da Posta in arrivo da inviare al dispositivo BlackBerry
In base all'impostazione predefinita di MDaemon, i messaggi contenuti nelle cartelle IMAP diverse da Posta in arrivo possono essere inviate alla posta in arrivo dello smartphone BlackBerry. Queste impostazioni si trovano nella schermata Posta in arrivo BlackBerry 352 dell'editor di account e nella pagina Cartelle di WorldClient. Tali schermate consentono, rispettivamente ad amministratori ed utenti, di selezionare le cartelle che contengono i nuovi messaggi da recapitare al dispositivo. Se non si desidera consentire ad alcun utente con dispositivi BlackBerry di raccogliere la posta da cartelle IMAP diverse da Posta in arrivo, disabilitare questa opzione. È consigliabile, tuttavia, lasciare questa opzione abilitata perché, in caso contrario, gli utenti che ordinano i messaggi in cartelle specifiche mediante i filtri IMAP 353 non saranno in grado di leggere sul proprio dispositivo i messaggi filtrati.

Questa funzione è indipendente dalle opzioni di integrazione dell'account delle schermate Domini[186] e Account integrati[188]. Anche se l'integrazione BIS di MDaemon viene disabilitata, gli utenti possono creare un account di posta elettronica sul proprio dispositivo BlackBerry per raccogliere la posta da MDaemon, esattamente come con qualsiasi altro client di posta elettronica tradizionale o smartphone. Questa funzione consente semplicemente agli utenti dello smartphone BlackBerry di raccogliere i messaggi dalle cartelle gestite con i filtri IMAP.

Attiva creazione alias cartella Posta inviata/eliminata per utenti BlackBerry
Per impostazione predefinita, uno schema per la gestione degli alias delle cartelle interne consente di assegnare alle cartelle "Posta inviata" e "Posta eliminata" di ogni utente valori riconosciuti da BIS, indipendentemente dal nome assegnato alle cartelle nell'account dell'utente. Ciò non altera in alcun modo i nomi delle cartelle. SI tratta di una funzione interna per la creazione di alias che consente di collocare la posta inviata ed eliminata nelle cartelle di MDaemon appropriate. Analogamente all'opzione precedente, anche questa è indipendente dalle opzioni di integrazione degli account. È possibile utilizzarla anche se l'opzione *Attiva integrazione BIS (BlackBerry Internet Service)* della schermata Domini è disabilitata. Se non si desidera creare alias delle cartelle per gli utenti BlackBerry, disabilitare questa opzione.

Nella pagina Cartelle di WorldClient è possibile indicare le cartelle da utilizzare per la Posta inviata e la Posta eliminata.

Applica Collegamento allegati agli account integrati BlackBerry
Selezionare questa casella di controllo per applicare la funzione Collegamento allegati[154] a tutti i messaggi inviati agli Account integrati[188] BlackBerry. Per applicare tale funzione, è necessario che la funzione *Attiva collegamento allegati* della finestra di dialogo Collegamento allegati sia attiva.

Consenti a più BlackBerry di integrarsi con lo stesso account MDaemon
Questa opzione consente di integrare più dispositivi BlackBerry con lo stesso account MDaemon. In questo modo, ad esempio, chi dispone di due smartphone BlackBerry può impostare i dispositivi in modo che ricevano entrambi la posta inviata all'account dell'utente.

Registra attività IMAP BIS (le attività vengono visualizzate nella scheda registro BIS)
Questa casella di controllo consente di registrare l'attività IMAP BIS. L'attività viene copiata nei file di registro e viene visualizzata nella scheda BIS della GUI principale.

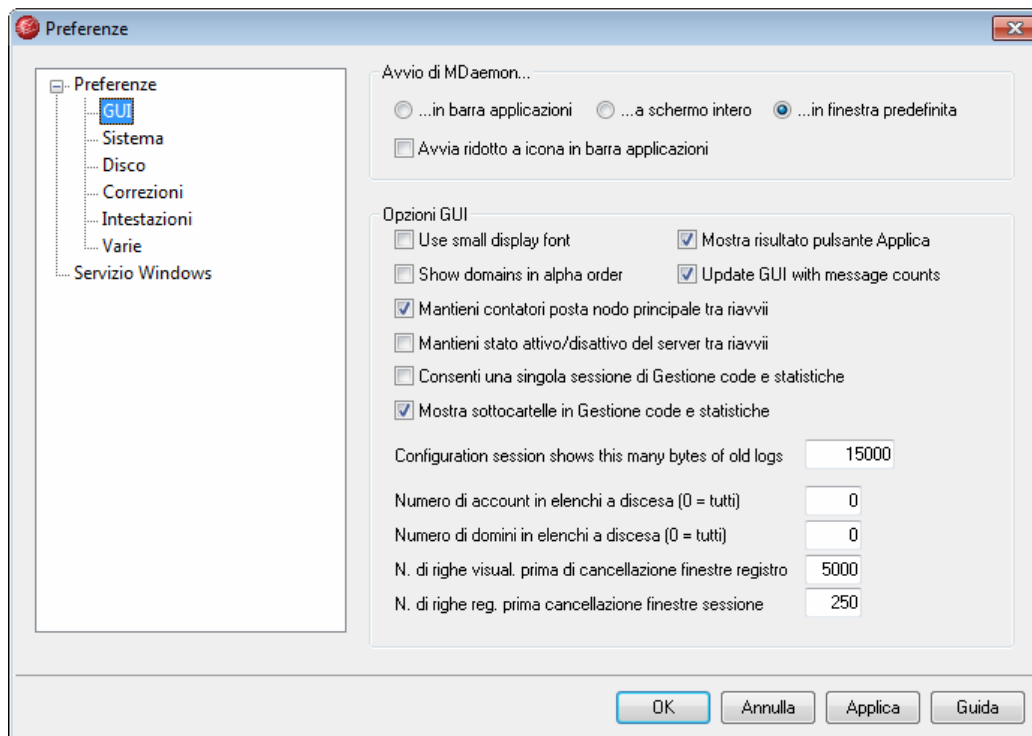
Registra notifiche complete dai server BIS (utile per il debug)
Questa casella di controllo consente di registrare tutte le attività dei server BIS. È un'opzione utile per il debug, perché contribuisce a diagnosticare i problemi relativi a BIS.

Vedere:

BIS BlackBerry 184
BIS BlackBerry » Domini 186
BIS BlackBerry » Account integrati 188
Account Editor » BIS BlackBerry 352

4.6 Preferenze

4.6.1 Preferenze

4.6.1.1 GUI

Avvio di MDaemon

...in barra applicazioni
Questa opzione consente di non visualizzare l'interfaccia di MDaemon all'avvio. L'icona di MDaemon, tuttavia, verrà comunque visualizzata nella barra delle applicazioni.

...a schermo intero
Selezionare questa opzione per ingrandire l'interfaccia di MDaemon all'avvio.

...in finestra predefinita
Selezionare questa opzione per visualizzare l'interfaccia di MDaemon in una finestra

predefinita all'avvio.

Avvia ridotto a icona in barra applicazioni
Se questa opzione è selezionata, MDaemon verrà avviato ridotto a icona e verrà visualizzato sia nella barra delle applicazioni sia nell'area di notifica. Deselezionare questa casella di controllo se non si desidera che, una volta ridotto a icona, MDaemon venga visualizzato nella barra delle applicazioni di Windows ma solo nell'area di notifica.

Opzioni GUI

Usa caratteri piccoli nelle finestre registro
Scegliere questa opzione se si desidera che le informazioni esposte nelle finestre Monitoraggio eventi e Sessioni vengano visualizzate in caratteri piccoli.

Mostra risultato pulsante Applica
Per impostazione predefinita, quando si fa clic sul pulsante Applica di una finestra di dialogo, viene aperta una finestra di messaggio che conferma il salvataggio delle modifiche apportate alle impostazioni. Per applicare le modifiche senza visualizzare il messaggio, deselezionare questa casella.

Elenca in ordine alfabetico i domini
Questa opzione consente di visualizzare in ordine alfabetico l'elenco dei domini nell'interfaccia principale di MDaemon. Se si deseleziona questa opzione, i domini verranno elencati nell'ordine con il quale vengono visualizzati nel file `domains.dat` della directory `\app\` di MDaemon. Quando si modifica questa impostazione, il nuovo metodo di ordinamento non verrà applicato fino al successivo riavvio di MDaemon.

Aggiornamento continuo dei conteggi dei messaggi
Questa opzione consente di controllare il disco per contare i messaggi in attesa nelle code di posta.

Mantieni contatori posta nodo principale tra riavvii
Abilitare questa opzione se si desidera salvare i valori dei contatori del nodo principale tra i riavvii del server. I contatori del nodo principale sono elencati nella sezione "Statistiche" del riquadro Statistiche di MDaemon.

Conserva lo stato attivo/inattivo del server tra i riavvii
Selezionare questa casella di controllo per garantire che lo stato (abilitato/ disabilitato) dei server di MDaemon non subisca variazioni dopo il riavvio.

Consenti una singola sessione di Gestione code e statistiche
Selezionare questa casella di controllo per eseguire una singola copia di Gestione code e statistiche 492 alla volta. Se si tenta di avviare il programma di gestione quando ne è già in esecuzione un'istanza, viene attivata la finestra relativa a quest'ultima.

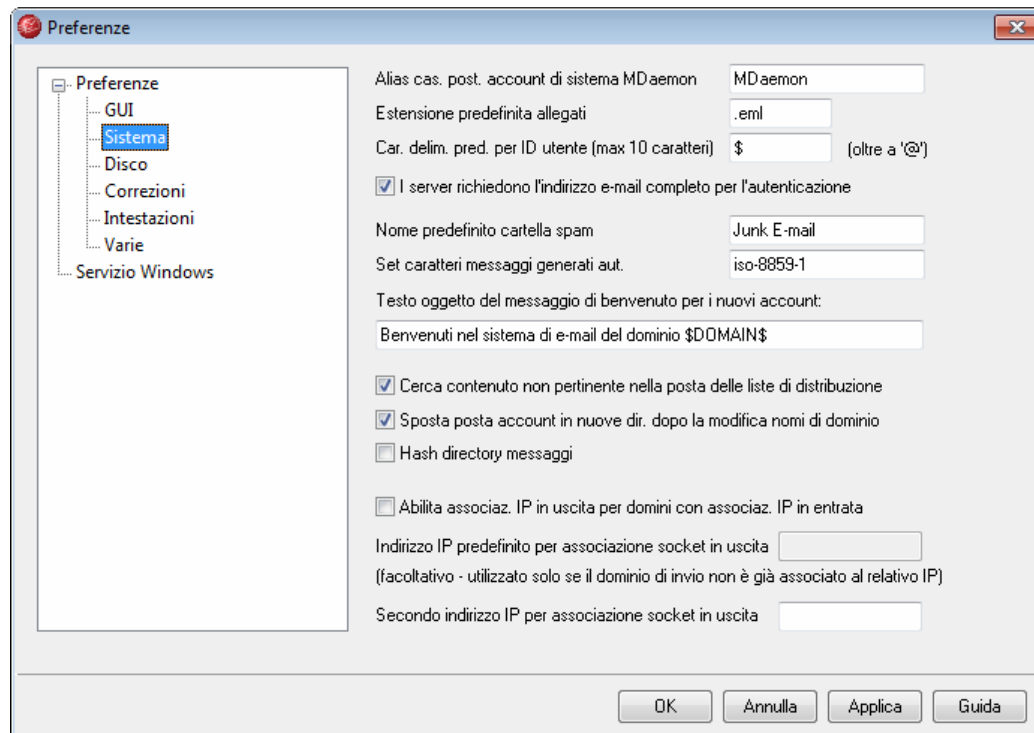
Mostra sottocartelle in Gestione code e statistiche
Selezionare questa casella di controllo per visualizzare le sottocartelle contenute nelle varie code e cartelle della posta degli utenti di Gestione code e statistiche 492.

Numero di account in elenchi a discesa (0 = tutti)
Rappresenta il numero massimo di account visualizzati negli elenchi a discesa delle varie finestre di dialogo. Se, inoltre, il valore di questa opzione è inferiore al numero degli account esistenti, non è più possibile visualizzare le opzioni "Modifica account" ed "Elimina account" del menu Account. Per modificare o eliminare gli account sarà necessario utilizzare Account Manager340. Per rendere effettive le modifiche apportate a questa opzione, riavviare MDaemon. L'impostazione predefinita è "0", che determina la visualizzazione di tutti gli account.

Numero di domini in elenchi a discesa (0 = tutti)
Indica il numero massimo di domini aggiuntivi visualizzati nella GUI principale, indipendentemente dalla quantità dei domini esistenti. Per rendere effettive le modifiche apportate a questo valore, riavviare MDaemon. L'impostazione predefinita è "0", che determina la visualizzazione di tutti i domini.

N. di righe visual. prima di cancellazione finestre registro
Indica il numero massimo di righe visualizzate nelle finestre di registro della visualizzazione principale. Il contenuto della finestra viene cancellato ogni volta che viene raggiunto questo numero di righe, senza influire sul file di registro, in quanto viene cancellata solo la visualizzazione.

N. di righe reg. prima cancellazione finestre sessione
Indica il numero massimo di righe visualizzate nella finestra Sessione35 prima della cancellazione. La cancellazione non influisce sul file di registro.

4.6.1.2 Sistema

Alias cas. post. account di sistema MDaemon [indirizzo]
In questo campo è riportato l'indirizzo e-mail da cui provengono i messaggi generati dal sistema. I messaggi di sistema includono le conferme di iscrizione, i messaggi DSN (Delivery Status Notification, notifica dello stato della consegna), altri tipi di messaggi di notifica e così via.

Estensione predefinita allegati
In questo campo è indicata l'estensione dei messaggi generati dal sistema. Tale estensione viene utilizzata anche per gli allegati inclusi nei messaggi generati dal sistema. Ad esempio, se MDaemon genera un avviso per il postmaster relativo a un messaggio specifico, all'avviso verrà allegato il messaggio con l'estensione specificata in questo campo.

Car. delim. pred. per ID utente (max 10 caratteri)
Se l'ID utente dell'account corrisponde all'indirizzo e-mail, è possibile utilizzare questo carattere o stringa di caratteri in alternativa al simbolo "@". L'opzione può rivelarsi necessaria se i client e-mail degli utenti non supportano il carattere "@" nel campo ID utente. Ad esempio, se il carattere immesso in questo campo è "$", gli utenti possono connettersi sia con "utente@dominio.com", sia con "utente$dominio.com".

I server richiedono l'indirizzo e-mail completo per l'autenticazione
Per accedere a MDaemon, i server POP e IMAP richiedono, per impostazione predefinita, l'indirizzo di posta elettronica completo. Per consentire l'accesso con la sola casella postale, ad esempio "franco" invece di "franco@esempio.com", disabilitare questa opzione, sebbene questo non sia consigliabile poiché l'accesso con la sola casella postale è ambiguo se MDaemon serve più domini.

Nome predefinito cartella spam
Inserire in questa casella di testo il nome predefinito della cartella spam che MDaemon creerà automaticamente per gli utenti. Il nome predefinito è "Junk E-mail" che corrisponde al valore predefinito di numerosi altri prodotti molto diffusi.

Set caratteri messaggi generati aut.
Specificare in questo campo il set caratteri da utilizzare per i messaggi generati automaticamente. L'impostazione predefinita è iso-8859-1.

Testo oggetto del messaggio di benvenuto per i nuovi account
MDaemon invia automaticamente un messaggio di benvenuto ai nuovi account. Il testo verrà visualizzato come intestazione "Subject" (Oggetto) del messaggio. l messaggio di benvenuto viene creato in base al file `NEWUSERHELP.DAT` della cartella `…\MDaemon\app\`. In questa intestazione possono essere incluse tutte le macro consentite negli script di risposta automatica 390.

Cerca contenuto non pertinente nella posta delle liste di distribuzione
Selezionare questa casella di controllo se si desidera scartare i messaggi indirizzati alle liste di distribuzione che in realtà dovrebbero essere indirizzati all'account di sistema. Ad esempio, per iscriversi a una lista o per annullare l'iscrizione, un utente inserisce all'inizio di un messaggio e-mail il comando Subscribe o Unsubscribe e lo invia all'indirizzo di sistema, ad esempio "mdaemon@esempio.com". Spesso questi

messaggi e-mail vengono inviati alla lista stessa per errore. Selezionare questa casella di controllo per evitare l'invio di questi messaggi alla lista.

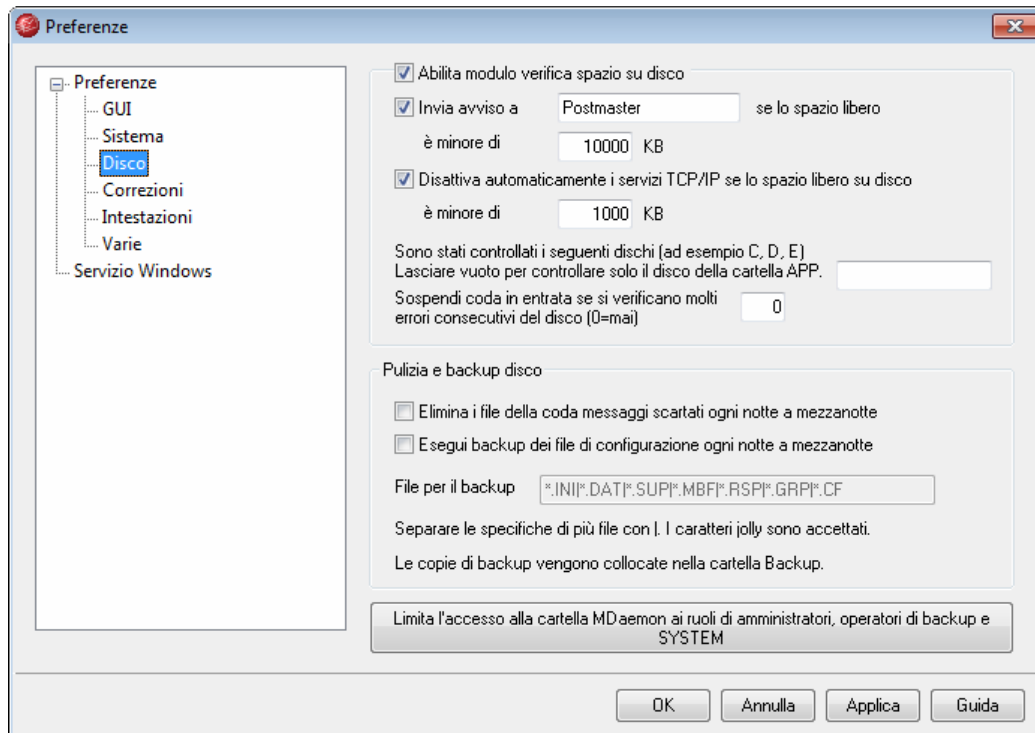
Sposta posta account in nuove dir. dopo la modifica nomi di dominio
Se questa opzione è selezionata, quando si rinomina un dominio la posta degli account del dominio viene spostata nelle directory con il nuovo nome. In caso contrario, MDaemon continuerà a utilizzare i nomi delle directory di posta precedenti.

Hash directory messaggi
Selezionare questa casella di controllo per abilitare l'hashing della directory. MDaemon eseguirà l'hashing di alcune directory creando fino a 65 sottocartelle. La procedura di hashing consente di migliorare le prestazioni di siti particolarmente voluminosi, ma può ridurre quelle dei siti MDaemon tradizionali. L'opzione è disabilitata per impostazione predefinita.

Abilita associaz. IP in uscita per domini con associaz. IP in entrata
Se si seleziona questa opzione, i domini che utilizzano l'opzione *Associa i socket in ascolto all'IP* utilizzano anche l'associazione ai socket in uscita. L'indirizzo IP utilizzato, se non diversamente specificato, è quello associato alla gestione della posta in entrata.

Indirizzo IP predefinito per associazione socket in uscita
Indirizzo IP che verrà utilizzato per l'associazione ai socket in uscita. Questa impostazione è facoltativa ed è necessaria solo nel caso in cui il dominio del mittente non sia già associato ai suoi indirizzi IP.

Secondo indirizzoIP per associazione socket in uscita
Specificare in questo campo l'eventuale indirizzo IP aggiuntivo da associare ai socket in entrata del dominio predefinito.

4.6.1.3 Disco

Abilita modulo verifica spazio su disco
Selezionare questa casella di controllo per attivare il monitoraggio dello spazio disponibile su disco per l'unità su cui è in esecuzione `MDaemon.exe`.

Invia avviso a [utente o indirizzo] se lo spazio libero è minore su di [xx] KB
Selezionare questa opzione per inviare a un utente o indirizzo un messaggio di notifica in cui si segnala che lo spazio su disco disponibile è inferiore a una determinata soglia.

Disattiva automaticamente i servizi TCP/IP se lo spazio libero su disco è minore di [xx] KB
Selezionare questa casella per disabilitare i servizi TCP/IP quando lo spazio disponibile su disco è inferiore a una determinata soglia.

Sono stati controllati i seguenti dischi (ad esempio C, D, E)
Questa opzione consente di monitorare lo spazio disponibile in più dischi, specificando la lettera di ciascuna unità. Se lasciata vuota, viene controllato solo il disco contenente la cartella `\app\` di MDaemon.

Sospendi coda in entrata se si verificano molti errori consecutivi del disco (0=mai)
Se durante l'elaborazione della coda in entrata si verifica il numero di errori del disco indicato, MDaemon interrompe l'elaborazione della coda fino a quando la condizione non viene risolta. L'interruzione viene notificata con un messaggio e-mail alla casella postale del postmaster.

Pulizia e backup disco

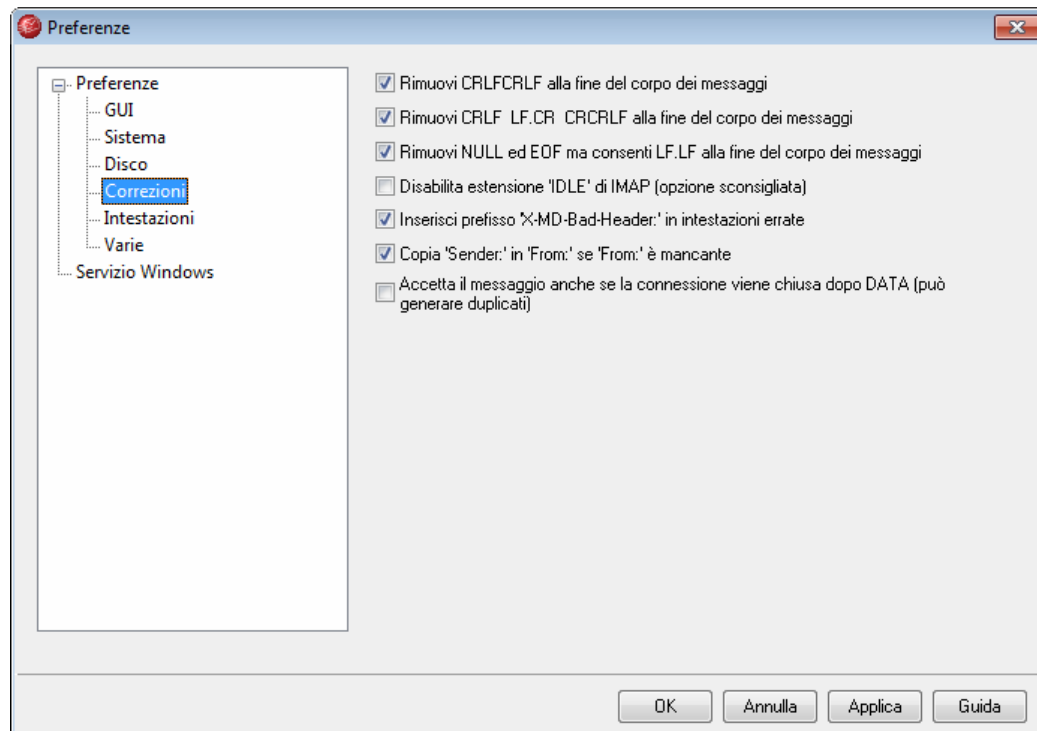
Elimina i file della coda messaggi scartati ogni notte a mezzanotte
Selezionare questa casella di controllo se si desidera che MDaemon elimini tutti i file dalla coda dei messaggi scartati ogni notte a mezzanotte. Questa funzione consente di risparmiare spazio su disco.

Esegui backup dei file di configurazione ogni notte a mezzanotte
Selezionare questa casella di controllo per archiviare tutti i file di configurazione di MDaemon ogni notte a mezzanotte nella directory Backups.

File per il backup
Specificare nella casella di testo i file e le estensioni dei file di cui si desidera effettuare il backup. I caratteri jolly sono consentiti. È necessario separare ogni nome di file o estensione con il carattere "|".

Limita l'accesso alla cartella MDaemon ai ruoli di ammministratori, operatori di backup e SYSTEM

Questo pulsante consente di limitare l'accesso alla cartella principale di `\MDaemon\` e alle relative sottocartelle ai seguenti account/gruppi di Windows: Administrators, Backup Operators e SYSTEM.

4.6.1.4 Correzioni

Rimuovi CRLFCRLF alla fine del corpo dei messaggi
Determinati client di posta possono presentare problemi nella visualizzazione dei messaggi che si concludono con più caratteri CRLF consecutivi. Quando si abilita questa casella, MDaemon elimina le sequenze `CRLFCRLF` consecutive al termine del corpo del messaggio. L'opzione è abilitata per impostazione predefinita.

Rimuovi CRLF LF.CR CRCRLF alla fine del corpo dei messaggi
Per impostazione predefinita, MDaemon rimuove questa sequenza alla fine dei messaggi, in quanto potrebbe determinare problemi con alcuni client di posta. Per non eliminare questa sequenza dai messaggi, disabilitare questa casella.

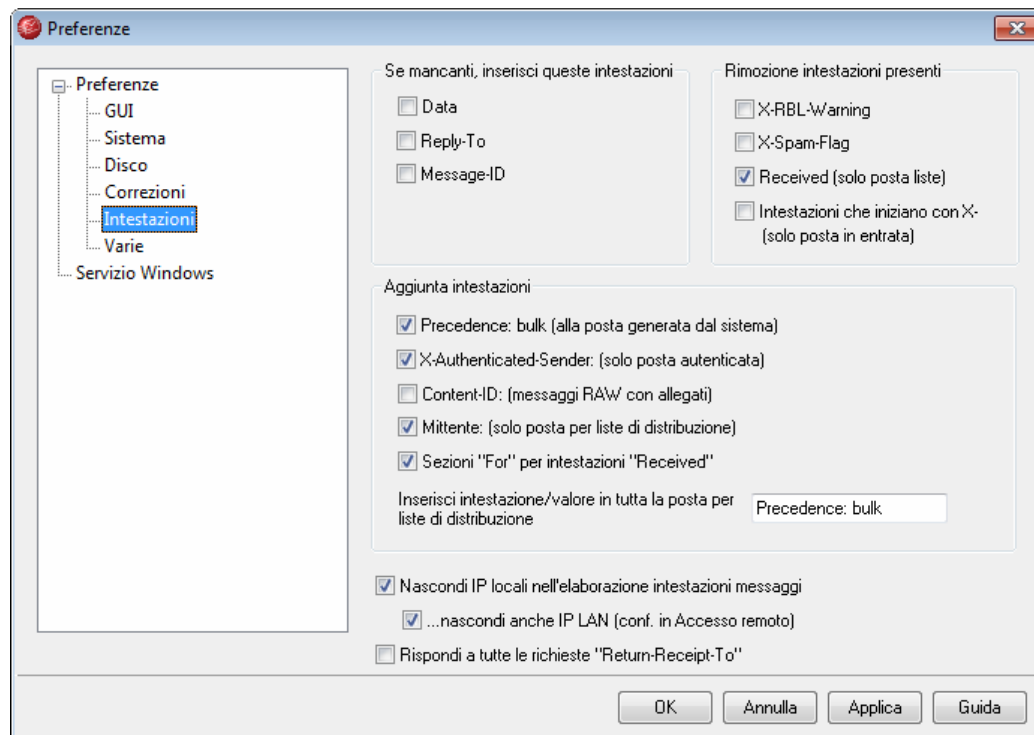
Rimuovi NULL ed EOF ma consenti LF.LF alla fine del corpo dei messaggi
Quando si abilita questa casella di controllo, MDaemon rimuove i caratteri `Null` ed EOF dalla fine del corpo dei messaggi, ma accetta i messaggi che terminano con `LF.LF`, nonché quelli che terminano con una normale sequenza `CRLF.CRLF` che indica la fine del messaggio. L'opzione è abilitata per impostazione predefinita.

Disabilita estensione 'IDLE' di IMAP (opzione sconsigliata)
Alcuni client di posta non aggiornati determinano problemi con l'estensione `IMAP IDLE`. Disabilitare il supporto di MDaemon per questa estensione non è consigliabile, ma è possibile farlo con questa opzione. Se gli utenti incontrano problemi relativi a questa estensione, abilitare la casella per disabilitare il supporto IMAP IDLE.

Inserisci prefisso "X-MD-Bad-Header:" in intestazioni errate
Quando si abilita questa opzione e MDaemon incontra un'intestazione errata, le antepone il prefisso "`X-MD-Bad-Header:`" L'opzione è abilitata per impostazione predefinita.

Copia 'Sender:' in 'From:' se 'From:' è mancante
Con alcuni client di posta non è possibile creare l'intestazione `FROM:` durante la composizione del messaggio. Le informazioni dell'intestazione `FROM:` vengono collocate, invece, nell'intestazione `Sender:`. Questo problema costituisce una fonte di confusione per alcuni server di posta e per il destinatario del messaggio. Per prevenire questi problemi, se si abilita questa casella, MDaemon crea l'intestazione `FROM:` mancante a partire dal contenuto dell'intestazione `Sender:`. L'opzione è abilitata per impostazione predefinita.

Accetta il messaggio anche se la connessione viene chiusa dopo DATA (può generare duplicati)
Se si abilita questa opzione, MDaemon accetta e consegna i messaggi anche se la connessione si interrompe durante o subito dopo il comando `DATA` nel corso dell'elaborazione SMTP. Questa opzione non dovrebbe essere utilizzata normalmente, poiché può condurre alla duplicazione di messaggi.

4.6.1.5 Intestazioni

Se mancanti, inserisci queste intestazioni

Date
Se si abilita questa opzione, in presenza di un messaggio privo dell'intestazione "`Date:`", MDaemon ne crea una e la aggiunge al file del messaggio. Il valore dell'intestazione corrisponde alla data di ricezione del messaggio, non a quella di creazione. Questa funzione consente di consegnare i messaggi inviati da client di posta che non creano le intestazioni relative alla data e che di norma non vengono accettati da alcuni server di posta.

Reply-To
Se si abilita questa opzione, in presenza di un messaggio privo dell'intestazione "`Reply-To`", MDaemon ne crea una e la aggiunge al file del messaggio utilizzando l'indirizzo dell'intestazione "`From`". Se l'intestazione "`Reply-To`" è presente, ma **vuota**, MDaemon crea l'intestazione: `Reply-To:` "". In questo modo, è possibile risolvere il problema per alcuni client di posta.

Message-ID
In presenza di un messaggio privo dell'intestazione "`Message-ID`", MDaemon ne crea una e la inserisce nel messaggio.

Rimozione intestazioni presenti

X-RBL-Warning
Abilitare questa casella di controllo per rimuovere tutte le intestazioni "`X-RBL-Warning:`" dai messaggi. L'opzione è disabilitata per impostazione predefinita.

X-Spam-Flag
Abilitare questa opzione se si desidera eliminare le intestazioni "X-Spam-Flag:" obsolete dai messaggi.

Received (solo posta liste)
Abilitare questa casella di controllo per eliminare tutte le intestazioni "Received:" esistenti dai messaggi della lista di distribuzione.

Intestazioni che iniziano con X- (solo posta in entrata)
Per inoltrare la posta ed eseguire alcune altre funzioni, MDaemon e altri server di posta utilizzano numerose intestazioni specifiche dette di tipo X. Se questa opzione è abilitata, MDaemon elimina queste intestazioni dai messaggi in entrata. **Nota:** con questa opzione non vengono rimosse le intestazioni X-RBL-Warning.

Aggiunta intestazioni

Precedenza: bulk (alla posta generata dal sistema)
Se si abilita questa casella, viene inserita un'intestazione "Precedence: bulk" in tutti i messaggi generati dal sistema, ad esempio messaggi di benvenuto, avvisi, messaggi che segnalano difficoltà di consegna e così via.

X-Authenticated-Sender: (solo posta autenticata)
Per impostazione predefinita, MDaemon aggiunge l'intestazione "X-Authenticated-Sender:" ai messaggi pervenuti mediante una sessione autenticata con il comando AUTH. Per evitare che venga aggiunta questa intestazione, disabilitare questa casella.

Content-ID: (messaggi RAW con allegati)
Selezionare questa casella di controllo per aggiungere intestazioni Content-ID MIME univoche ai messaggi creati da un file RAW contenente allegati.

Mittente: (solo posta liste di distribuzione)
Questa opzione consente di inserire l'intestazione Sender nei messaggi delle liste di distribuzione. **Nota:** dal momento che l'intestazione Sender è obbligatoria per la firma DomainKeys della lista dei messaggi, questa opzione non ha effetto quando MDaemon è stato configurato per la firma DomainKeys, in quanto tutta la posta della lista deve disporre di un'intestazione Sender.

Sezioni 'For' per intestazioni 'Received:'
Fare clic su questa opzione se si desidera che le sezioni "For [destinatario SMTP]" vengano aggiunte all'intestazione "Received:" del messaggio aggiunto da MDaemon.

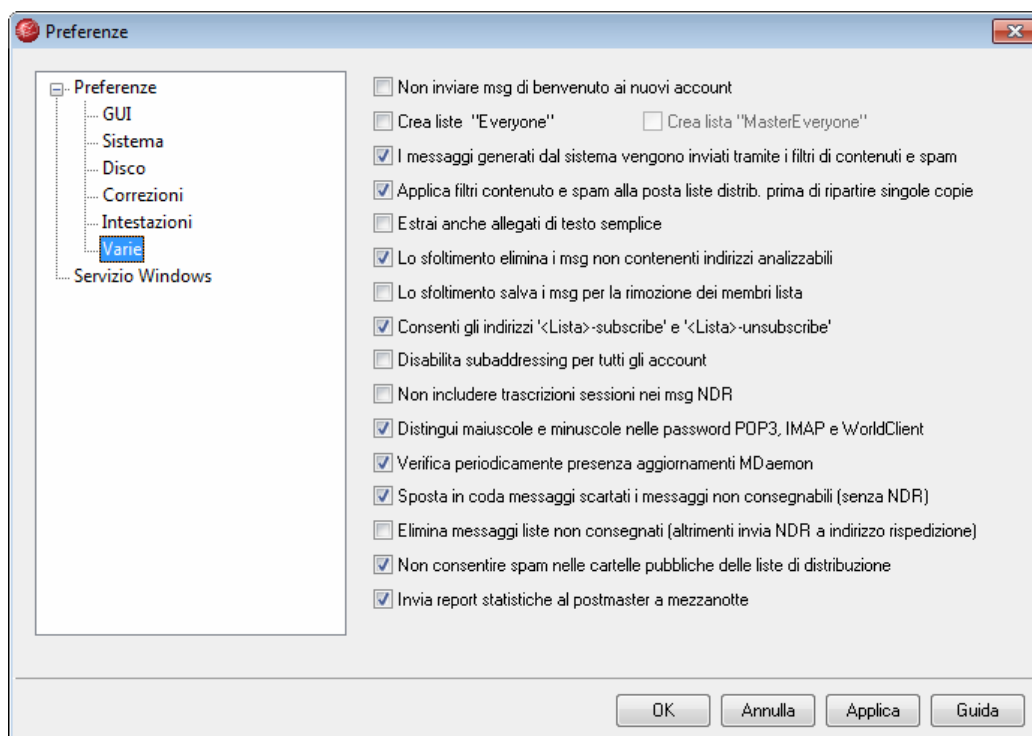
Inserisci intestazione/valore in tutta la posta per liste di distribuzione[intestazione**]**
È possibile specificare una combinazione statica intestazione/valore, ad esempio "Precedence: bulk", per tutti i messaggi delle liste di distribuzione.

-

Nascondi IP locali nell'elaborazione intestazioni messaggi
Selezionare questa casella per impedire a MDaemon di inserire gli indirizzi IP locali nelle intestazioni dei messaggi durante l'elaborazione della posta.

...nascondi anche IP LAN (conf. in Accesso remoto)
Se MDaemon è configurato per nascondere gli indirizzi IP locali, selezionare questa casella di controllo per nascondere anche gli indirizzi IP inclusi nella schermata IP LAN 100.

Rispondi a tutte le richieste 'Return-Receipt-To:'
Selezionare questa casella di controllo per soddisfare le richieste di conferma dell'avvenuta consegna dai messaggi in entrata e inviare automaticamente un messaggio di conferma al mittente. L'opzione è disabilitata per impostazione predefinita.

4.6.1.6 Varie

Non inviare msg di benvenuto ai nuovi account
In base all'impostazione predefinita, MDaemon genera un messaggio di benvenuto basato sul file `NEWUSERHELP.DAT` e lo distribuisce ai nuovi utenti quando viene creato il relativo account. Selezionare questa casella di controllo per impedire la generazione di tale messaggio.

Crea liste "Everyone"
Se si abilita questa casella di controllo, MDaemon crea e gestisce liste di distribuzione "Everyone" per i domini, ad esempio "everyone@esempio.com".

L'aggiornamento delle liste di distribuzione di ciascun utente su tutti i domini di MDaemon costituisce un potenziale spreco di risorse, se tali liste non vengono mai utilizzate o sono destinate a un elevatissimo numero di utenti. L'opzione è disabilitata per impostazione predefinita.

Crea lista "MasterEveryone"
Questa opzione consente di ottenere una lista di distribuzione "MasterEveryone". In questo modo, in questa lista saranno inclusi tutti coloro che sono presenti in tutte le liste "Everyone" del dominio specifico. L'opzione è disabilitata per impostazione predefinita.

I messaggi generati dal sistema vengono inviati mediante il Filtro contenuti
Per impostazione predefinita, i messaggi generati dal sistema vengono elaborati mediante Filtro contenuti. Per escluderli da Filtro contenuti, disabilitare la casella di controllo.

Applica filtri contenuto e spam alla posta liste distrib. prima di ripartire singole copie
Quando si seleziona l'opzione *MDaemon ripartisce posta lista* della schermata Instradamento dell'editor delle liste di distribuzione, l'abilitazione di questo controllo determina l'applicazione delle regole di Filtro contenuti e di Spam Filter ai messaggi della lista prima che vengano ripartiti e distribuiti ai singoli membri.

Estrai anche allegati di testo semplice
Per impostazione predefinita, l'estrazione automatica degli allegati non interessa gli allegati di tipo `text/plain` (testo semplice). Selezionare questa casella di controllo se si desidera estrarre automaticamente anche questo tipo di allegato.

Lo sfoltimento elimina i messaggi non contenenti indirizzi analizzabili
Quando MDaemon è configurato per analizzare i messaggi restituiti alle liste di distribuzione al fine di cancellare gli iscritti non raggiungibili, questa opzione consente di eliminare i messaggi che non contengono un indirizzo analizzabile. Per ulteriori informazioni, vedere il comando *Rimuovi automaticamente gli indirizzi inattivi dalla lista dei membri* della schermata Membri dell'editor delle liste di distribuzione.

Lo sfoltimento salva i msg per la rimozione dei membri lista
Quando MDaemon è configurato per analizzare i messaggi restituiti alle liste di distribuzione allo scopo di eliminare gli iscritti non raggiungibili, la selezione di questa opzione consente di salvare i messaggi provenienti da iscritti rimossi dalla lista.

Consenti gli indirizzi '<Lista>-subscribe' e '<Lista>-unsubscribe'
Selezionare questa casella di controllo se si desidera che MDaemon riconosca come validi (purché la lista esista) gli indirizzi e-mail con questo formato, al fine di fornire agli utenti un metodo più semplice per iscriversi o ritirarsi dalle liste di distribuzione. Ad esempio: si supponga di avere una lista di nome `NomeLista@altn.com`. Gli utenti possono iscriversi/ritirarsi dalla lista inviando un messaggio e-mail agli indirizzi `NomeLista-Subscribe@altn.com` e `NomeLista-Unsubscribe@altn.com`. Il contenuto dell'oggetto e del corpo del messaggio è irrilevante. Inoltre, quando questa funzione è attiva, MDaemon inserisce in tutti i messaggi della lista l'intestazione seguente:

```
List-Unsubscribe: <mailto:<Lista>-Unsubscribe@domain.com>
```

Alcuni client e-mail sono in grado di convertire automaticamente questa intestazione in un pulsante ANNULLA ISCRIZIONE disponibile agli utenti.

Disabilita subaddressing per tutti gli account
Selezionare questa opzione se si desidera disabilitare a livello globale la funzionalità subaddressing. Tale funzionalità verrà quindi disattivata per tutti gli account, indipendentemente dalle impostazioni dei singoli account. Per ulteriori informazioni sulla funzionalità subaddressing, vedere la schermata Filtri IMAP 353 di Account Editor.

Non includere trascrizioni sessioni nei messaggi NDR
Selezionare questa casella di controllo per escludere le trascrizioni delle sessioni SMTP dai messaggi di avviso e di segnalazione di errore nel recapito.

Distingui maiuscole e minuscole nelle password POP3, IMAP e WorldClient
Se questa casella di controllo è selezionata, nelle password POP, IMAP e WorldClient si farà distinzione tra lettere maiuscole e minuscole.

Verifica periodicamente presenza aggiornamenti MDaemon
Se questa casella di controllo è selezionata, MDaemon verificherà regolarmente la disponibilità di aggiornamenti software. Quando è disponibile una nuova versione, verrà inviato un messaggio di notifica e sarà possibile scaricare e installare l'aggiornamento, se desiderato.

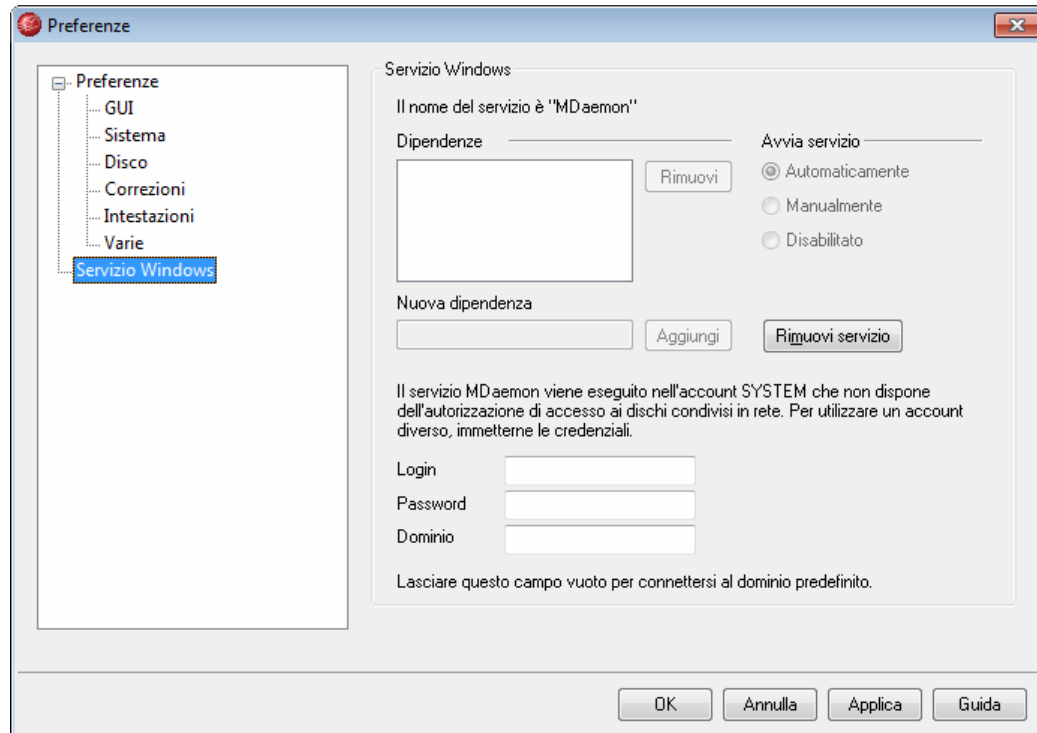
Sposta in coda messaggi scartati i messaggi non consegnabili (senza NDR)
Quando si abilita questa opzione, i messaggi inoltrati con i quali si siano verificati errori di consegna permanenti e irreversibili o i messaggi scaduti della coda tentativi vengono spostati nella coda messaggi scartati, senza che il mittente originale riceva un messaggio NDR (Non-Delivery Receipt, ricevuta di mancato recapito). Disabilitando questa opzione, il mittente originale riceve un messaggio NDR. L'opzione è abilitata per impostazione predefinita.

Elimina messaggi liste non consegnati (altrimenti invia NDR a indirizzo rispedizione)
Quando si abilita questa opzione, i messaggi della lista di distribuzione con i quali si siano verificati errori di consegna permanenti e irreversibili o i messaggi scaduti della coda tentativi vengono eliminati, senza che venga generato alcun messaggio NDR. Disabilitando questa opzione, all'*Indirizzo di rispedizione SMTP* 442 indicato viene restituito un messaggio NDR. L'opzione è disabilitata per impostazione predefinita.

Non consentire spam nelle cartelle pubbliche delle liste di distribuzione
Per impostazione predefinita, quando a una lista di distribuzione viene associata una cartella pubblica 445, i messaggi della lista non vengono collocati nella cartella se il punteggio di spam raggiunge o supera il valore indicato nell'opzione "*Il msg è di spam se il punteggio è > o = a*" che si trova nella schermata Spam Filter 244. Per consentire l'inserimento dei messaggi spam nella cartella pubblica, disabilitare questa casella di controllo.

Invia report statistiche al postmaster a mezzanotte
Per impostazione predefinita, il report statistiche viene inviato al postmaster ogni notte a mezzanotte. Deselezionare questa casella se non si desidera che il report venga inviato. Questa opzione corrisponde alla scheda Statistiche 30 situata nella

visualizzazione principale di MDaemon.

4.6.2 Servizio Windows

Servizio Windows

Se MDaemon viene eseguito come servizio, il nome del servizio è "MDaemon".

Dipendenze
Questa opzione consente di indicare i servizi che devono essere in esecuzione **prima** dell'avvio del servizio MDaemon.

Avvia servizio
Indica lo stato iniziale del servizio: avvio automatico, avvio manuale o disabilitato.

Installa/Rimuovi servizio
Per installare o rimuovere il servizio MDaemon, fare clic su questo pulsante.

Accesso alle risorse di rete

Per impostazione predefinita, MDaemon viene eseguito come servizio di sistema nell'ambito dell'account SYSTEM. Poiché tale account non ha accesso alle periferiche di rete, MDaemon non è in grado di accedere alla posta se questa si trova su altri computer della rete LAN. Per risolvere questo problema, è sufficiente fornire le credenziali di connessione di un account che consenta al servizio MDaemon di accedere alle condivisioni di rete. In questo caso è possibile creare un account utente Windows specifico per l'esecuzione di MDaemon, contenente tutte le restrizioni necessarie e

l'accesso alle condivisioni di rete che devono essere disponibili per MDaemon. Tutte le applicazioni avviate da MDaemon utilizzeranno le stesse credenziali.

Login
Indica il nome dell'ID utente dell'account Windows nel cui ambito viene eseguito il servizio MDaemon.

Password
È la password dell'account Windows.

Dominio
Indica il dominio Windows al quale appartiene l'account. Per connettersi al dominio predefinito, lasciare questo campo vuoto.

Sezione V

5 Menu Sicurezza

MDaemon dispone di una suite completa di funzioni e di comandi di sicurezza. Fare clic su Sicurezza nella barra dei menu di MDaemon per accedere alle funzioni di sicurezza illustrate di seguito:

- **AntiVirus** 211 - SecurityPlus per MDaemon consente di arrestare la ricezione di virus via e-mail fornendo il maggior livello possibile di protezione integrata per i clienti di MDaemon. Questo sistema cattura, pone in quarantena, pulisce e/o elimina tutti i messaggi e-mail rivelatisi infetti. La funzione Protezione attacchi (Outbreak Protection, OP) di SecurityPlus, disponibile solo per la versione MDaemon PRO, offre ulteriori funzioni di protezione da spam, da virus e da attacchi di tipo phishing talvolta non individuati dalle misure di protezione tradizionali, basate sul contenuto dei messaggi e sulle definizioni dei virus.
- **Filtro contenuti** 212 - Un sistema di filtro dei contenuti molto versatile e totalmente multi-thread consente di personalizzare il comportamento del server in base al contenuto dei messaggi e-mail in entrata e in uscita. È possibile inserire e aggiungere intestazioni di messaggio, aggiungere piè di pagina ai messaggi, rimuovere gli allegati, inoltrare copie ad altri utenti, attivare l'invio automatico di un messaggio istantaneo, eseguire programmi e altro ancora.
- **Spam Filter** 243 - Una nuova tecnologia di filtro dei messaggi spam per esaminare, tramite un procedimento euristico, i messaggi e-mail calcolando un "punteggio". Questo viene usato per determinare la probabilità che un messaggio sia di tipo spam. In base al punteggio, il server può intraprendere determinate azioni, ad esempio respingendo il messaggio o contrassegnandolo. Vedere anche: Spam Trap 273
- **Liste nere DNS** 267 - Questa funzione consente di specificare numerosi servizi di gestione di liste nere DNS che vengono consultati ogni volta che un messaggio viene inviato al server MDaemon. Se l'indirizzo IP che richiede la connessione è presente sulla lista nera di uno qualsiasi di questi host, il messaggio viene respinto.
- **Controllo inoltro** 274 - Questa funzione consente di controllare il comportamento di MDaemon quando al server viene recapitato un messaggio in cui né il mittente né il destinatario sono indirizzi locali.
- **Scudo IP** 276 - Questa funzione consente la connessione al server solo se l'indirizzo IP del nome di dominio che richiede la connessione è presente in questo elenco.
- **Autenticazione SMTP** 283 - Questa funzione consente di impostare diverse opzioni che controllano il comportamento di MDaemon nel caso in cui un utente che invia un messaggio è già stato precedentemente autenticato o nel caso inverso.
- **Ricerca inversa** 278 - Questa funzione consente di interrogare i server DNS per verificare la validità dei nomi di dominio e degli indirizzi riportati nei messaggi in entrata. I comandi di questa schermata consentono di respingere i messaggi dubbi o di inserirvi un'intestazione speciale. I dati di Ricerca inversa vengono inoltre riportati nei registri di MDaemon.
- **Verifica POP prima di SMTP** 281 - I comandi di questa schermata consentono di

obbligare ogni utente ad accedere alla propria casella postale prima di poter inviare un messaggio mediante MDaemon. In questo modo, l'utente viene autenticato come titolare di un account valido e viene autorizzato a utilizzare il sistema di posta.

- **Host accreditati** 282 - Questa funzione elenca i nomi di dominio e gli indirizzi IP associati a eccezioni delle regole di inoltro specificate nella scheda Impostazioni di inoltro.
- **SPF/ID mittente** 285 - Tutti i domini pubblicano i record MX per identificare i sistemi che possono ricevere posta per essi, ma questa funzione non è in grado di identificare le posizioni consentite per l'invio. SPF (Sender Policy Framework) e ID mittente sono mezzi attraverso i quali i domini possono anche pubblicare i record "MX inversi" per identificare le posizioni che sono autorizzate a inviare messaggi.
- **DomainKeys e DomainKeys Identified Mail** 287 - DK (DomainKeys) e DKIM (DomainKeys Identified Mail) sono sistemi di verifica della posta elettronica utilizzati per prevenire lo "spoofing" o contraffazione. Tali sistemi possono essere usati anche per garantire l'integrità dei messaggi in arrivo o per assicurarsi che il messaggio non sia stato alterato nell'intervallo di tempo trascorso dal momento in cui ha lasciato il server di posta del mittente al momento in cui è arrivato a destinazione. Ciò è possibile grazie all'uso di un sistema di coppie di chiavi pubbliche o private crittografate. I messaggi in uscita vengono firmati usando una chiave privata mentre i messaggi in arrivo dispongono di proprie firme verificate controllandole con una chiave pubblica pubblicata sul server DNS del mittente.
- **Certificazione** 298 - Nel processo di certificazione dei messaggi, un'entità garantisce o "certifica" la correttezza del comportamento relativo alla posta elettronica tenuto da un'altra entità. La certificazione rappresenta un vantaggio perché consente di evitare l'applicazione delle funzionalità di analisi antispam a messaggi per i quali non è necessaria, nonché di ridurre le risorse necessarie per l'elaborazione di ciascun messaggio.
- **Lista nera indirizzi** 304 - Questa funzione elenca gli indirizzi non autorizzati a inviare posta attraverso il server.
- **Vaglio IP** 305 - Questa funzione è utilizzata per specificare gli indirizzi IP ai quali accordare o rifiutare le connessioni al server.
- **Vaglio host** 307 - Questa funzione è utilizzata per specificare gli host (nomi di dominio) ai quali consentire o rifiutare le connessioni al server.
- **Vaglio dinamico** 309 - Utilizzando le funzioni di vaglio dinamico, MDaemon è in grado di tenere traccia del comportamento dei server di invio per identificare attività sospette e rispondere di conseguenza. Ad esempio, con il vaglio automatico, è possibile escludere momentaneamente un indirizzo IP da future connessioni al server, a seguito di un determinato numero di errori per "destinatario sconosciuto" verificatisi da quell'indirizzo durante la connessione di posta.
- **SSL e TLS** 311 - MDaemon include il supporto del protocollo SSL (Secure Sockets Layer) per SMTP, POP, IMAP e per il server Web di WorldClient. SSL è il metodo standard per la protezione delle comunicazioni Web tra server e client.
- **Protezione backscatter** 323 - Il termine "Backscatter" si riferisce ai messaggi di

risposta ricevuti dagli utenti relativi a messaggi mai spediti. Ciò si verifica quando i messaggi spam o i messaggi inviati da virus includono un indirizzo di ritorno contraffatto. Questa funzionalità utilizza un metodo di codifica hash di una chiave privata per generare e inserire nell'indirizzo del percorso di ritorno dei messaggi in uscita uno speciale codice con validità temporale limitata, in modo da consentire la ricezione dei soli messaggi di risposta automatica e di notifica di recapito legittimi.

- **Regolazione larghezza di banda** 326 - La funzionalità di regolazione della larghezza di banda è una nuova funzione che consente di controllare la larghezza di banda utilizzata da MDaemon. È possibile controllare la velocità di avanzamento delle sessioni o dei servizi, impostando velocità diverse per ogni servizio principale di MDaemon in base al dominio, compresi il dominio predefinito, i domini aggiuntivi e i gateway di dominio.
- **Tarpitting** 329 - Questa funzione consente di rallentare deliberatamente una connessione a seguito della ricezione di un determinato numero di comandi RCPT dal mittente. Ciò consente di scoraggiare l'invio di messaggi e-mail non desiderati. L'assunto che sottende a questa tecnica consiste nell'imporre ai mittenti di messaggi indesiderati un periodo di attesa lungo e variabile per l'invio di ogni messaggio, scoraggiandoli così nel ritentare l'operazione.
- **Greylisting** 331 - È una tecnica antispam che sfrutta il fatto che i server SMTP ritentano la consegna di qualsiasi messaggio riceva un codice di errore temporaneo del tipo "riprovare più tardi". Utilizzando questa tecnica, durante la sessione SMTP i messaggi che provengono da un mittente non inserito nella lista bianca o semplicemente sconosciuto vengono rifiutati con un codice di errore temporaneo e il mittente, il destinatario e l'indirizzo IP del server di invio vengono registrati. Quando i server legittimi tentano di recapitare nuovamente i messaggi alcuni minuti più tardi, questi vengono accettati. Dal momento che gli "spammer" in genere non eseguono ulteriori tentativi di consegna, questa funzione consente di ridurre considerevolmente il numero di messaggi spam ricevuti.
- **HashCash** 334 - È un sistema basato su "prove" e può essere considerato sia uno strumento antispam sia una contromisura contro attacchi di tipo DoS (Denial-of-Service), concettualmente analogo a un metodo di affrancatura elettronica. Grazie al sistema HashCash, MDaemon è in grado di "coniare" dei contrassegni HashCash, per i quali, in realtà, si "paga" in tempi di elaborazione della CPU anziché in moneta. Il contrassegno HashCash viene inserito nelle intestazioni dei messaggi in uscita e poi verificato dal server e-mail del destinatario e stimato in base al valore del contrassegno. La probabilità che i messaggi contrassegnati siano legittimi è maggiore, per questo tali messaggi possono superare i sistemi antispam del server ricevente.
- **IP LAN** 336 - In questa schermata vengono elencati gli indirizzi IP presenti sulla rete LAN in uso. Per quanto attiene alla regolazione della larghezza di banda, tali indirizzi IP vengono considerati come locali e possono essere esclusi da varie altre limitazioni di sicurezza e antispam.
- **Criteri sito** 337 - Questa funzione consente di creare i criteri di utilizzo del sito da trasmettere ai server di invio all'inizio di ogni sessione di posta SMTP. Un esempio comune di criterio di utilizzo del sito potrebbe essere il seguente: "Questo server non provvede all'inoltro."

5.1 Filtro contenuti e antivirus

Filtro contenuti

La schermata Filtro contenuti 212, accessibile selezionando Sicurezza » Filtro contenuti, consente di configurare una vasta gamma di funzioni per prevenire la posta indesiderata, intercettare i messaggi contenenti virus prima che raggiungano la destinazione finale, copiare specifici messaggi e-mail per uno o più utenti aggiuntivi, inserire una nota o una clausola alla fine dei messaggi, aggiungere ed eliminare le intestazioni, rimuovere gli allegati, cancellare i messaggi e così via. Poiché vengono create dall'amministratore, le regole di Filtro contenuti possono essere di molti tipi e applicabili alle situazioni più diverse. Se progettata e sperimentata con accortezza, questa funzione può rivelarsi molto utile.

SecurityPlus per MDaemon

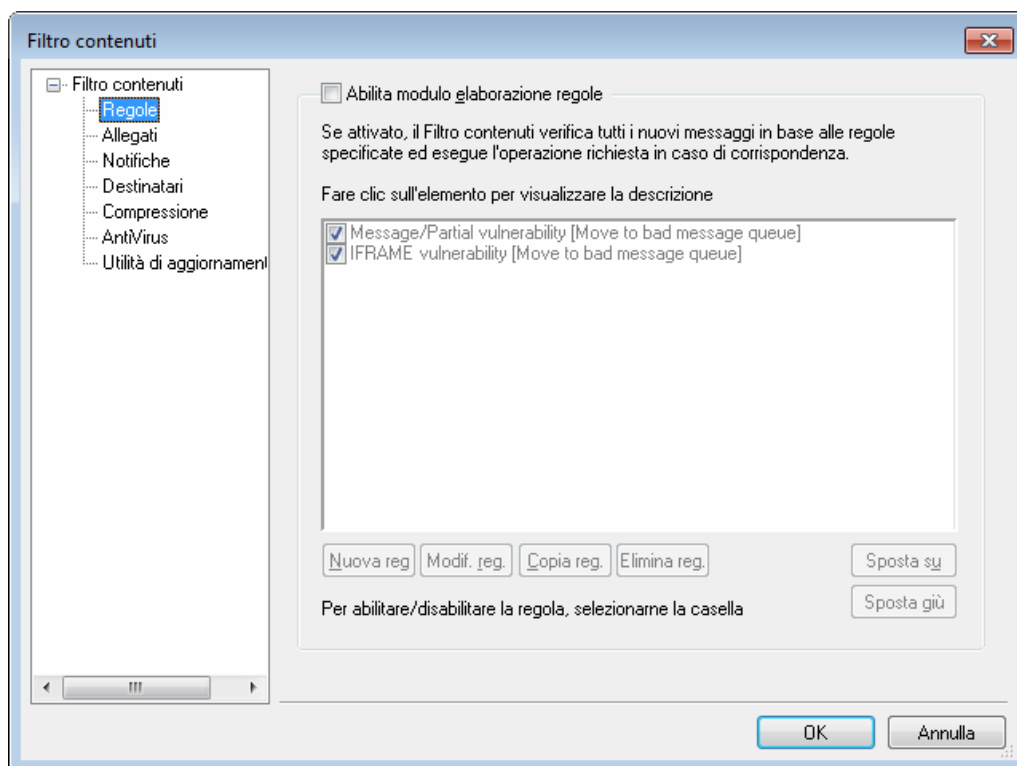
Questo strumento di individuazione dei virus che può essere integrato con MDaemon è nato dalla collaborazione tra Kaspersky Labs, che sviluppa soluzioni antivirus conosciute a livello mondiale, e Alt-N Technologies. Dopo l'installazione di SecurityPlus, la finestra di dialogo Filtro contenuti visualizza due schede aggiuntive: AntiVirus 232 e Utilità di aggiornamento AV 235. Queste consentono di controllare direttamente le funzioni del prodotto e di specificare le operazioni da eseguire quando viene rilevato un virus. Per gli utenti di MDaemon PRO, SecurityPlus include inoltre una funzione chiamata Protezione attacchi 238 (OP, Outbreak Protection) che, a differenza dei tradizionali strumenti di protezione basati su algoritmi euristici o su file di definizione dei virus, è stata appositamente progettata per intercettare messaggi spam, virus e attacchi di tipo phishing relativi a un attacco in corso, talvolta non individuati dagli strumenti di concezione tradizionale. Per ottenere SecurityPlus per MDaemon, visitare il sito www.altn.com.

Per ulteriori informazioni, vedere:

Filtro contenuti 212
Creazione di una nuova regola di filtro dei contenuti 214
Modifica di una regola di Filtro contenuti esistente 219
Uso di espressioni regolari nelle regole di filtro 219

AntiVirus 232
Utilità di aggiornamento AntiVirus 235
Protezione attacchi 238

5.1.1 Editor di Filtro contenuti

5.1.1.1 Regole

Ogni messaggio elaborato da MDaemon viene temporaneamente collocato in una delle code dei messaggi. Se la funzione Filtro contenuti è abilitata, ogni messaggio dovrà essere elaborato dalle regole di Filtro contenuti prima di poter lasciare la coda. Il risultato di questa procedura determina il destino del messaggio.

I messaggi con nome file che inizia con la lettera "P" vengono ignorati dal processo di Filtro contenuti. Tutti gli altri vengono invece elaborati in base a tale sistema. Al termine

dell'elaborazione, il primo carattere del nome file dei messaggi viene sostituito con la lettera "P", in modo che il contenuto di ogni messaggio venga filtrato una sola volta.

Regole del filtro contenuti

Abilita modulo elaborazione regole
Selezionare questa casella di controllo per abilitare Filtro contenuti. Prima di essere consegnati, tutti i messaggi elaborati da MDaemon verranno filtrati mediante le regole di Filtro contenuti.

Elenco delle regole di Filtro contenuti

La casella di testo include tutte le regole di Filtro contenuti, ognuna associata a una casella di controllo che consente di abilitarla o disabilitarla. Per visualizzare una descrizione di ciascuna regola in base al formato script interno, selezionare la regola e attendere senza spostare il cursore del mouse per evitare di far scomparire la descrizione. Quando un messaggio viene elaborato da Filtro contenuti, le regole vengono applicate nell'ordine in cui sono elencate. L'ordine può essere modificato per ottenere un grado di flessibilità maggiore.

Ad esempio: se si dispone di una regola che impone l'eliminazione di tutti i messaggi contenenti le parole "Questa è posta indesiderata" e di una regola simile che causa l'invio di questi messaggi al postmaster, per poter applicare entrambe le regole al messaggio sarà sufficiente disporle nell'ordine appropriato. A questo scopo è necessario che in una posizione superiore all'interno dell'elenco non sia stata applicata la regola "STOP processing rules (Blocca elaborazione regole)". Altrimenti, occorrerà utilizzare i pulsanti *Sposta su*/*Sposta giù* per posizionare la regola di interruzione dopo le altre due. Ogni messaggio contenente "Questa è posta indesiderata" verrà copiato e inviato al postmaster, quindi eliminato.

MDaemon consente di creare regole per effettuare più operazioni e di utilizzare gli operatori logici `and/or`. Nell'esempio precedente, anziché utilizzare più regole, sarebbe stato possibile eseguire tutte le operazioni con un'unica regola.

Nuova regola
Fare clic su questo pulsante per creare una nuova regola di Filtro contenuti. Verrà visualizzata la finestra di dialogo Crea regola 214.

Modifica regola
Fare clic su questo pulsante per visualizzare la regola selezionata nell'editor modifica regola 219.

Copia regola
Fare clic su questo pulsante per duplicare la regola di Filtro contenuti selezionata. Verrà creata e aggiunta all'elenco una regola identica a quella selezionata. Alla nuova regola viene automaticamente assegnato il nome predefinito "Copia di [nome della regola originale]". L'opzione si rivela particolarmente utile per creare più regole

simili. È infatti sufficiente creare una singola regola, duplicarla più volte, quindi modificare le copie a seconda delle esigenze.

Elimina regola
Fare clic su questo pulsante per eliminare la regola di Filtro contenuti selezionata. Verrà chiesto di confermare l'eliminazione.

Sposta su
Fare clic su questo pulsante per spostare la regola selezionata verso l'alto.

Sposta giù
Fare clic su questo pulsante per spostare la regola selezionata verso il basso.

Per ulteriori informazioni, vedere:

Creazione di una nuova regola di Filtro contenuti 214
Modifica di una regola di Filtro contenuti esistente 219
Uso di espressioni regolari nelle regole di filtro 219

5.1.1.1.1 Creazione di una nuova regola di Filtro contenuti

La finestra di dialogo Crea regola consente di definire le regole di Filtro contenuti. Per visualizzarla, fare clic sul pulsante *Nuova regola* nella finestra di dialogo di Filtro contenuti.

Crea regola

Nome della regola
Digitare in questo campo un nome descrittivo da assegnare alla nuova regola. Per impostazione predefinita, la regola viene denominata "New Rule #n (Nuova regola n.)".

Condizioni

In questa casella vengono elencate le condizioni da applicare alla nuova regola. Selezionare la casella di controllo corrispondente alla condizione da applicare alla nuova regola. Ogni condizione abilitata verrà visualizzata nella sottostante casella di descrizione della regola. Per specificare le informazioni aggiuntive necessarie per la maggior parte delle condizioni, fare clic sul collegamento ipertestuale della condizione nella casella di descrizione della regola.

If the [HEADER] contains (Se l'intestazione [INTESTAZIONE] contiene) - Fare clic su una di queste opzioni per costruire la regola in base al contenuto dell'intestazione di messaggio selezionata. È necessario specificare il testo da ricercare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 219.

If the user defined [# HEADER] contains (Se l'intestazione [INTESTAZIONE #] definita dall'utente contiene) - Fare clic su una o più di queste opzioni per costruire la regola in base a intestazioni di messaggio personalizzate. È necessario specificare la nuova intestazione e il testo da ricercare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 219.

If the MESSAGE BODY contains (Se il CORPO DEL MESSAGGIO contiene) - Questa opzione trasforma il corpo del messaggio in una nelle condizioni. È necessario specificare la stringa di testo da cercare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 219.

If the MESSAGE has Attachment(s) (Se il MESSAGGIO ha allegati) - Se questa opzione è selezionata, la regola dipenderà dalla presenza di uno o più allegati. Non è necessario fornire informazioni aggiuntive.

If the MESSAGE SIZE is greater than (Se la DIMENSIONE DEL MESSAGGIO supera) - Selezionare questa opzione per creare la regola in base alla dimensione del messaggio. La dimensione deve essere indicata in *KB*. L'impostazione predefinita è 10 KB.

If the MESSAGE HAS A FILE called (Se il MESSAGGIO INCLUDE UN FILE denominato) - Se questa opzione è selezionata, verrà eseguita la ricerca di un allegato con un nome particolare. Il nome del file deve essere specificato. Sono

consentiti i caratteri jolly, ad esempio, *.exe e *.*.

If message is INFECTED (Se il messaggio è INFETTO) - Questa condizione restituisce TRUE se SecurityPlus individua la presenza di un virus in un messaggio.

If the EXIT CODE from a previous run process is equal to (Se il CODICE DI USCITA del programma precedente è uguale a) - Se in una regola precedente dell'elenco viene utilizza l'azione *Esegui processo*, sarà possibile avvalersi di questa condizione per cercare un determinato codice di uscita dal programma.

If the MESSAGE IS DIGITALLY SIGNED (Se il MESSAGGIO CONTIENE UNA FIRMA DIGITALE) - La condizione viene applicata ai messaggi provvisti di firma digitale. Non è necessario aggiungere ulteriori informazioni.

If SENDER is a member of GROUP (Se il MITTENTE appartiene al GRUPPO) - La condizione viene applicata ai messaggi inviati da un account appartenente al gruppo specificato nella regola.

If RECIPIENT is a member of GROUP (Se il DESTINATARIO appartiene al GRUPPO) - La condizione viene applicata ai messaggi i cui destinatari appartengono al gruppo di account specificato nella regola.

If ALL MESSAGES (Se TUTTI I MESSAGGI) - Selezionare questa opzione per applicare la regola a tutti i messaggi. Non è necessario aggiungere ulteriori informazioni. Questa regola ha effetto su tutti i messaggi, eccezione fatta per quelli a cui è stata applicata l'azione "Blocca elaborazione regole" o "Elimina messaggio" nell'ambito di una regola precedente.

Azioni

Consente di specificare le azioni da eseguire se un messaggio corrisponde alle condizioni della regola. Per alcune azioni sono necessarie informazioni aggiuntive, che possono essere specificate facendo clic sul collegamento ipertestuale relativo all'azione nella casella di descrizione della regola.

Delete Message (Elimina messaggio) - Se viene selezionata questa azione, il messaggio verrà eliminato.

Strip All Attachments From Message (Rimuovi tutti gli allegati dal messaggio) - Se viene selezionata questa azione, gli allegati del messaggio verranno rimossi.

Move Message To Bad Message Directory (Sposta il messaggio in directory messaggi scartati) - Se viene selezionata questa azione, il messaggio verrà spostato nella directory dei messaggi scartati.

Skip n Rules (Ignora n regole) - Se viene selezionata questa azione, verrà ignorato il numero di regole specificato. L'opzione è utile per applicare la regola in

alcune circostanze ma non in altre.

Ad esempio: si supponga di voler eliminare i messaggi contenenti le parole "Pubblicità non desiderata", ma non quelli contenenti le parole "Pubblicità gradita". A tale scopo, è necessario creare una regola in base alla quale eliminare i messaggi contenenti le parole "Pubblicità non desiderata" e, in una posizione superiore nell'elenco delle regole, specificare una regola che stabilisce di ignorare la prima se il messaggio contiene le parole "Pubblicità gradita".

Stop Processing Rules (Blocca elaborazione regole) - Questa azione consente di ignorare tutte le regole successive.

Copy Message To Specified User(s) (Invia copia messaggio agli utenti specificati) - Se viene selezionata questa azione, una copia del messaggio verrà inviata a uno o più destinatari. È necessario specificare i destinatari del messaggio.

Append Standard Disclaimer (Aggiungi nota standard) - Questa azione consente di creare un breve testo da aggiungere come piè di pagina al messaggio. In alternativa, è possibile aggiungere il contenuto di un file di testo.

Ad esempio: questa regola è utile per includere il testo "Questo messaggio e-mail è stato inviato da nomeazienda. Per commenti o domande, scrivere a utente@nomeazienda.com".

Add Extra Header Item To Message (Aggiungi intestazione al messaggio) - Questa opzione consente di aggiungere un'intestazione al messaggio. È necessario specificare il nome e il valore della nuova intestazione.

Delete A Header Item From Message (Elimina intestazione dal messaggio) - Questa azione consente di rimuovere un'intestazione dal messaggio. È necessario specificare l'intestazione da eliminare.

Send Note To (Invia una nota a) - Questa azione consente di inviare un messaggio e-mail a un determinato indirizzo. Le opzioni disponibili consentono di specificare il destinatario, il mittente, l'oggetto e un breve testo. È inoltre possibile allegare alla nota il messaggio originale.

Ad esempio: è possibile creare una regola in base a cui tutti i messaggi contenenti il testo "Questa è posta indesiderata" devono essere spostati nella directory dei messaggi scartati e un'altra regola che consente di inviarne notifica all'utente.

Remove Digital Signature (Rimuovi firma digitale) - Questa azione consente di rimuovere una firma digitale dal messaggio.

Run Process (Esegui processo) - Questa azione è utile per eseguire un particolare programma quando un messaggio corrisponde alle condizioni della regola. È necessario specificare il percorso del programma da eseguire. È possibile utilizzare la macro $MESSAGEFILENAME$ per passare il nome del messaggio al processo, nonché

specificare se sospendere temporaneamente o indefinitamente le operazioni di MDaemon durante l'esecuzione. Inoltre, è possibile imporre la conclusione del processo e/o l'esecuzione in una finestra nascosta.

Send Message through SMS Gateway Server (Invia il messaggio mediante server gateway SMS) - Questa opzione consente di inviare il messaggio mediante un server gateway SMS. È necessario specificare l'host o l'indirizzo IP e il numero di telefono SMS.

Copy Message to Folder (Copia messaggio nella cartella) - Questa opzione consente di collocare una copia del messaggio in una cartella specifica.

MOVE the messages to custom QUEUE (SPOSTA i messaggi nella CODA personalizzata) - Questa azione consente di spostare il messaggio in una o più code di posta personalizzate esistenti. Se si spostano i messaggi nelle code di posta remota personalizzate, è possibile utilizzare le opzioni di pianificazione personalizzata di Pianificazione eventi per controllare il momento in cui i messaggi vengono elaborati.

Add Line To Text File (Aggiungi riga a file di testo) - Questa opzione consente di aggiungere una riga a uno specifico file di testo. È necessario specificare il percorso del file e il testo da aggiungere. Nel testo possono essere utilizzate alcune macro, in modo che Filtro contenuti includa dinamicamente informazioni quali il mittente, il destinatario, l'ID messaggio e così via. Per visualizzare l'elenco delle macro consentite, fare clic sul pulsante Macro nella finestra di dialogo "Aggiungi riga a file di testo".

Move Message to Public Folders (Sposta messaggio in cartelle pubbliche) - Questa azione consente di spostare il messaggio in una o più cartelle pubbliche.

Search and Replace Words within HEADER (Trova e sostituisci in un'intestazione) - Questa opzione consente di cercare determinate parole in un'intestazione specificata, quindi di eliminarle o sostituirle. Durante la creazione di questa regola, fare clic sul collegamento ipertestuale relativo alla specifica delle informazioni nella descrizione della regola per aprire la finestra "Intestazione – cerca e sostituisci", nella quale è possibile inserire l'intestazione e le parole da sostituire o eliminare. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 219.

Search and Replace within BODY (Trova e sostituisci nel corpo del messaggio) - Questa opzione consente di eseguire la scansione del corpo del messaggio per sostituire il testo desiderato. Questa condizione supporta ora espressioni regolari. Per ulteriori informazioni, vedere Uso di espressioni regolari nelle regole di filtro 219.

Jump to Rule (Vai a regola) - Questa opzione consente di passare immediatamente a una regola successiva nell'elenco, ignorando tutte le regole intermedie.

Sign with DomainKeys selector (Firma con il selettore DomainKeys) - Selezionando questa azione, nel messaggio verrà inserita una firma DomainKeys 293. L'azione consente anche di firmare alcuni messaggi con un selettore diverso da quello indicato nella finestra di dialogo DK & DKIM.

Sign with DKIM selector (Firma con il selettore DKIM) - Selezionando questa azione, nel messaggio verrà inserita una firma DKIM 293. L'azione consente anche di firmare alcuni messaggi con un selettore diverso da quello indicato nella finestra di dialogo DK & DKIM.

Descrizione regola
In questa casella viene visualizzato il formato script interno della nuova regola. Fare clic su una delle condizioni o azioni della' regola, rappresentate da collegamenti ipertestuali, per aprire l'editor appropriato e specificare le informazioni richieste.

Per ulteriori informazioni, vedere:

Editor di Filtro contenuti 212
Modifica di una regola di Filtro contenuti esistente 219
Uso di espressioni regolari nelle regole di filtro 219

5.1.1.1.2 Modifica di una regola di Filtro contenuti esistente

Per modificare una regola esistente, selezionarla e fare clic sul pulsante *Modifica regola* nella finestra di dialogo di Filtro contenuti. Verrà visualizzato l'editor che consente di modificare la regola. I comandi presenti in questo editor sono identici a quelli della finestra di dialogo Crea regola 214.

Per ulteriori informazioni, vedere:

Filtro contenuti 212
Creazione di una nuova regola di filtro dei contenuti 214
Uso di espressioni regolari nelle regole di filtro 219

5.1.1.1.3 Uso di espressioni regolari nelle regole di filtro

Il sistema di Filtro contenuti supporta le ricerche in base a *espressioni regolari*, una tecnica versatile che consente di cercare non solo stringhe di testo specifiche, ma anche *modelli* di testo. Le espressioni regolari contengono un insieme di testo semplice e di caratteri speciali che indicano il genere di corrispondenza da ricercare e, di conseguenza, rendono le regole di filtro dei contenuti più potenti e mirate.

Descrizione delle espressioni regolari
Un'espressione regolare (regular expression o regexp) è un modello di testo costituito da una combinazione di caratteri speciali, noti come *metacaratteri* e di caratteri di testo alfanumerici o "*letterali*", ad esempio abc, 123 e così via. Il modello viene utilizzato per confrontare le stringhe di testo. Le espressioni regolari vengono utilizzate

principalmente per individuare corrispondenze di testo normale e per eseguire ricerche e sostituzioni.

I metacaratteri sono caratteri speciali utilizzati per funzioni e scopi specifici nell'ambito delle espressioni regolari. L'implementazione delle espressioni regolari nel sistema Filtro contenuti di MDaemon consente l'utilizzo dei seguenti metacaratteri:

`\ | () [] ^ $ * + ? . <>`

Metacaratteri	Descrizione
****	Quando precede un metacarattere, la barra rovesciata ("\") fa sì che questo venga considerato come un carattere letterale. La barra è necessaria se si desidera che l'espressione regolare esegua la ricerca di uno dei caratteri speciali utilizzati come metacarattere. Ad esempio, per la ricerca di "+" le espressioni devono includere "\+".
|	Il carattere *disgiuntivo* (chiamato anche "*OR*" o "*barra verticale* ") viene utilizzato per indicare che una delle espressioni ai lati del carattere deve corrispondere alla stringa di destinazione. Nella ricerca di una stringa di testo, l'espressione regolare "abc|xyz" troverà una corrispondenza con tutte le occorrenze di "abc" o "xyz".
[...]	Una serie di caratteri tra parentesi quadre ("[" e "]") indica che qualsiasi carattere della serie può corrispondere alla stringa di testo desiderata. Un trattino ("-") interposto tra i caratteri racchiusi da parentesi indica un intervallo di caratteri. Ad esempio, la ricerca della stringa "abc" con l'espressione regolare "[a-z]" produrrà tre corrispondenze: "*a*", "*b*" e "*c*". L'utilizzo dell'espressione "[az]" determinerà una sola corrispondenza: "*a*".
^	Indica l'inizio di una riga. Nella stringa di destinazione "abc ab a", l'espressione "^a" produrrà una corrispondenza, ovvero il primo carattere della stringa di destinazione. Anche l'espressione regolare "^ab" produrrà una corrispondenza, con i primi *due* caratteri della stringa di destinazione.
[^...]	L'accento circonflesso ("^") immediatamente successivo alla parentesi quadra sinistra ("[") ha un altro significato. Viene utilizzato per escludere gli altri caratteri tra parentesi dalla corrispondenza con la stringa di destinazione. L'espressione "[^0-9]" indica che il carattere di destinazione non deve essere un numero.
(...)	Le parentesi interessano l'ordine di valutazione del modello e operano come espressione *racchiusa tra tag* da utilizzare per le espressioni di *ricerca e sostituzione*.

Il risultato di una ricerca eseguita con un'espressione regolare viene temporaneamente conservato e può essere utilizzato nell'espressione *sostitutiva* per creare una nuova espressione. Nell'espressione *sostitutiva*, è possibile includere un carattere "&" o "\0" che verrà sostituito dalla sottostringa individuata dall'espressione regolare durante la ricerca. Se l'espressione di *ricerca* "a(bcd)e" individua una corrispondenza con una sottostringa, l'espressione *sostitutiva* "123-&-123" o "123-\0-123" sostituirà il testo corrispondente con "123-abcde-123".

Analogamente, nell'espressione *sostitutiva* è possibile utilizzare anche i caratteri speciali "\1", "\2", "\3" e così via. Questi caratteri vengono sostituiti solo dai risultati dell'espressione *racchiusa tra tag* anziché dall'intera sottostringa corrispondente. Se l'espressione regolare contiene più espressioni racchiuse da tag, il numero che segue la barra rovesciata indica l'espressione racchiusa tra tag alla quale si fa riferimento. Ad esempio, se l'espressione di *ricerca* è "(123)(456)" e l'espressione *sostitutiva*è "a-\2-b-\1", la sottostringa corrispondente verrà sostituita con "a-456-b-123", mentre l'espressione *sostitutiva* "a-\0-b" verrà sostituita con "a-123456-b"

**$** Il simbolo di dollaro ("$") indica la fine della riga. Nella stringa di testo "13 321 123", l'espressione "3$" produrrà una corrispondenza, rappresentata dall'ultimo carattere della stringa. Anche l'espressione regolare "123$" produrrà una corrispondenza, con gli ultimi *tre* caratteri della stringa di destinazione.

***** L'asterisco ("*") di quantificazione indica che il carattere situato a sinistra deve corrispondere a *zero o più* occorrenze del carattere in una riga. Pertanto, "1*abc" produrrà una corrispondenza con il testo "111abc" e "abc".

+ Analogamente all'asterisco di quantificazione, il segno "+" di quantificazione indica che il carattere situato a sinistra deve corrispondere a *una o più* occorrenze del carattere in una riga. Pertanto, "1+abc" produrrà una corrispondenza con il testo "111abc", ma non con il testo "abc".

? Il punto interrogativo ("?") di quantificazione indica che il carattere situato a sinistra deve corrispondere *zero o una* volta. "1?abc" produrrà quindi una corrispondenza con il testo "abc" e con la porzione "1abc" di "111abc".

. Il metacarattere punto (".") indica una corrispondenza con qualsiasi altro carattere. ".+abc" produrrà una corrispondenza con "123456abc" e "a.c" con "aac", abc", acc" e così via.

Condizioni e azioni appropriate

È possibile utilizzare le espressioni regolari in qualsiasi *Condizione* della regola di filtro *Intestazione*. Ad esempio in qualsiasi regola la cui condizione sia "`If the FROM HEADER contains (Se l'INTESTAZIONE FROM contiene)`". Le espressioni regolari possono essere utilizzate anche nella condizione "`If the MESSAGE BODY contains (Se il CORPO DEL MESSAGGIO contiene)`".

Le espressioni regolari possono essere utilizzate in due *azioni* delle regole di Filtro contenuti: "`Search and Replace Words within HEADER (Trova e sostituisci in un'intestazione)`" e "`Search and Replace within BODY (Trova e sostituisci nel corpo del messaggio).`"

Le espressioni regolari utilizzate nelle *condizioni* delle regole di Filtro contenuti non tengono conto della distinzione tra maiuscole/minuscole. Una lettera maiuscola viene considerata identica alla stessa lettera minuscola.

Il riconoscimento di maiuscole e minuscole nelle espressioni regolari utilizzate nelle *azioni* delle regole di Filtro contenuti è facoltativo. Quando si crea un'espressione regolare nell'azione della regola, è possibile abilitare o disabilitare questa opzione.

Configurazione di un'espressione regolare nella condizione di una regola

Per configurare una condizione di intestazione o corpo del messaggio utilizzando un'espressione regolare, procedere come indicato di seguito.

1. Nella finestra di dialogo Crea regola, scegliere la casella di controllo corrispondente alla condizione di intestazione o corpo del messaggio da inserire nella regola.

2. Nell'area di riepilogo situata nella parte inferiore della finestra di dialogo Crea regola, scegliere il collegamento "**contains specific strings (contiene stringhe specifiche)**" corrispondente alla condizione selezionata nel passaggio 1. Verrà visualizzata la finestra di dialogo Specifica testo ricerca.

3. Fare clic sul collegamento "**contains (contiene)**" all'interno dell'area "Stringhe correnti".

4. Scegliere "**Matches Regular Expression (Corrisponde a espressione regolare)**" nella casella di riepilogo a discesa, quindi fare clic su **OK.**

5. Se si desidera assistenza per la creazione dell'espressione regolare o si intende controllarla, scegliere "**Prova espressione regolare**." Se non si desidera utilizzare la finestra di dialogo Test espressione regolare, inserire l'espressione regolare nella casella di testo, scegliere **Aggiungi** e proseguire con il passaggio 8.

6. Inserire l'espressione nella casella di testo "Cerca espressione". Per semplificare il processo, utilizzare il menu di scelta rapida, che consente di inserire agevolmente i metacaratteri desiderati nell'espressione. Per accedere al menu, scegliere il pulsante ">". Quando si seleziona un'opzione del menu, nell'espressione viene

inserito il metacarattere corrispondente e il punto di inserimento viene spostato nella posizione appropriata per il carattere stesso.

7. Digitare il testo per il controllo dell'espressione nell'area di testo e scegliere **Test.** Al termine del controllo, scegliere **OK.**

8. Fare clic su **OK.**

9. Proseguire con la creazione della regola.

Configurazione di un'espressione regolare nell'azione di una regola

Per configurare un'azione di ricerca e sostituzione utilizzando un'espressione regolare, attenersi alla procedura indicata di seguito.

1. Nella finestra di dialogo Crea regola, scegliere la casella di controllo corrispondente all'azione "*Search and Replace... (Trova e sostituisci)*" da inserire nella regola.

2. Nell'area di riepilogo situata nella parte inferiore della finestra di dialogo Crea regola, scegliere il collegamento "**specify information (specifica informazioni)**" corrispondente all'azione selezionata nel passaggio 1. Verrà visualizzata la finestra di dialogo Trova e sostituisci.

3. Se nel passaggio 1 si è scelta l'azione "*Search...header (Cerca in intestazione...)*", nella casella di riepilogo a discesa selezionare l'intestazione desiderata oppure digitarla, se non disponibile. In caso contrario, ignorare questo passaggio.

4. Inserire l'espressione di *ricerca* desiderata. Per semplificare il processo, utilizzare il menu di scelta rapida, che consente di inserire agevolmente i metacaratteri desiderati nell'espressione. Per accedere al menu, scegliere il pulsante ">". Quando si seleziona un'opzione del menu, nell'espressione viene inserito il metacarattere corrispondente e il punto di inserimento viene spostato nella posizione appropriata per il carattere stesso.

5. Inserire l'espressione *sostitutiva* desiderata. Come nel caso dell'espressione di *ricerca*, anche in questa situazione è possibile utilizzare un menu di scelta rapida. Per eliminare la sottostringa anziché sostituirla con un testo diverso, lasciare la casella di testo vuota.

6. Se si desidera che l'espressione tenga conto di maiuscole e minuscole, scegliere "**Maiuscole/minuscole**".

7. Per trovare e sostituire stringhe da considerare come espressioni regolari, scegliere Espressione regolare. In caso contrario, ogni stringa verrà considerata come semplice sottostringa di ricerca e sostituzione e verrà ricercata una corrispondenza letterale esatta del testo.

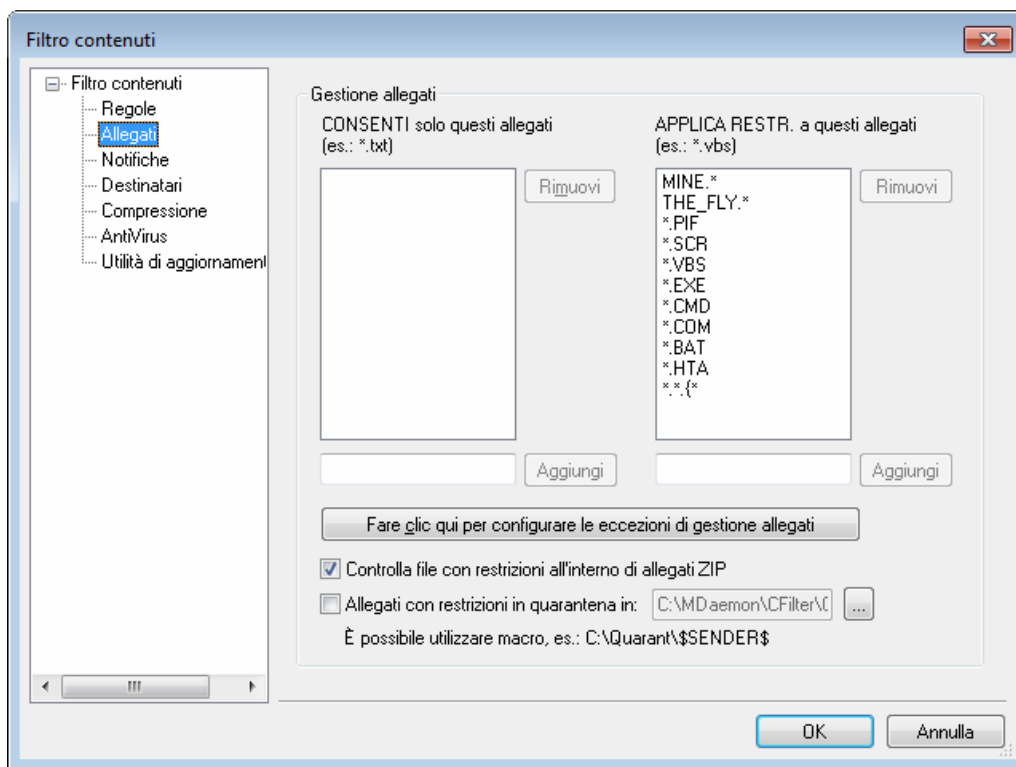
8. Se non si desidera controllare l'espressione, ignorare questo passaggio. Per controllare l'espressione, scegliere "**Esegui controllo.**" Nella finestra di dialogo relativa al controllo delle operazioni di ricerca e sostituzione, inserire le espressioni e il testo da controllare, quindi scegliere **Test.** Al termine del controllo, scegliere **OK** .

9. Fare clic su **OK.**

10. Proseguire con la creazione della regola.

Per l'implementazione delle espressioni regolari di MDaemon viene utilizzata la libreria PCRE (PERL Compatible Regular Expression). È possibile ottenere ulteriori informazioni sull'implementazione delle espressioni regolari visitando i seguenti indirizzi: http://www.pcre.org/ e http://perldoc.perl.org/perlre.html.

Per una descrizione esauriente delle espressioni regolari, consultare: *Mastering Regular Expressions, Terza edizione* pubblicato da O'Reilly Media, Inc (in lingua inglese).

5.1.1.2 Allegati

Questa scheda consente di specificare gli allegati da classificare come ammessi o con restrizioni. Gli allegati non consentiti vengono rimossi automaticamente dai messaggi.

Gestione allegati

I nomi file specificati nell'elenco *APPL. RESTRIZIONI a questi allegati* vengono rimossi automaticamente dai messaggi. Se si inseriscono file nell'elenco *CONSENTI solo questi allegati*, verranno ammessi solo i file presenti nell'elenco e tutti gli altri allegati

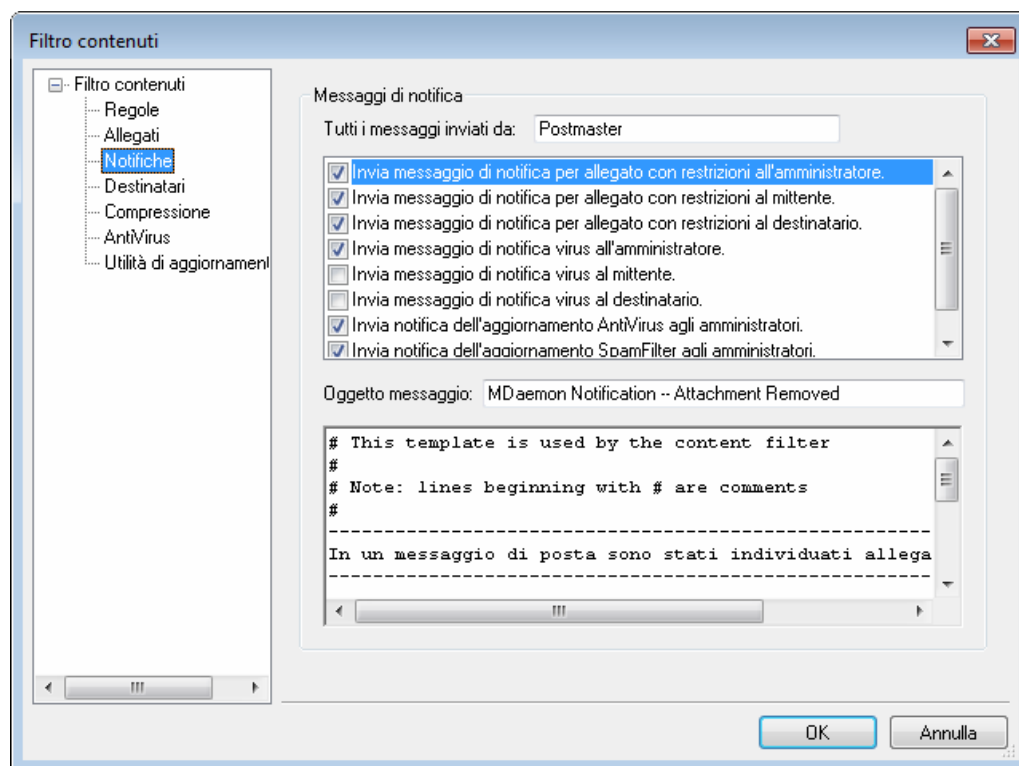
verranno rimossi. Dopo la rimozione dell'allegato, MDaemon consegna normalmente il messaggio, ma senza l'allegato. Le opzioni della scheda Notifiche possono essere utilizzate per inviare un messaggio di notifica a più indirizzi quando viene rilevato un allegato con restrizioni.

Nelle voci dell'elenco sono consentiti i caratteri jolly. Ad esempio, la voce "`*.exe`" determina l'ammissione o la rimozione di tutti gli allegati con estensione `EXE`. Per aggiungere una voce a un elenco, digitarne il nome file nell'apposito campo, quindi fare clic su Aggiungi.

Fare clic qui per configurare le eccezioni di gestione allegati
Fare clic su questo pulsante per specificare gli indirizzi da escludere dal controllo delle restrizioni imposte agli allegati. I messaggi destinati a questi indirizzi vengono elaborati anche se contengono un allegato con restrizioni.

Controlla file con restrizioni all'interno di allegati ZIP
Selezionare questa opzione se si desidera eseguire la scansione dei file compressi per individuare allegati con restrizioni al loro interno. Questa opzione, inoltre, consente di attivare eventuali regole di Filtro contenuti impostate per la ricerca di nomi file specifici qualora tali file vengano individuati in allegati compressi.

Allegati con restrizioni in quarantena in
Per porre in quarantena gli allegati con limitazioni in una posizione specifica anziché eliminarli, selezionare questa opzione e indicare la posizione desiderata.

5.1.1.3 Notifiche

Questa scheda consente di indicare i destinatari dei messaggi di notifica relativi al rilevamento di un virus o di un allegato con restrizioni.

Messaggi di notifica

Tutti i messaggi inviati da:
Questa casella consente di specificare l'indirizzo da cui inviare i messaggi di notifica.

Invia messaggio di notifica virus a...
Quando viene recapitato un messaggio con un allegato contenente un virus, viene inviato un messaggio di avviso ai soggetti specificati in questa sezione. È possibile inviare un messaggio personalizzato al mittente, al destinatario e agli amministratori specificati nella scheda Destinatari. Per personalizzare il messaggio per una qualsiasi di queste tre voci, selezionarne una dall'elenco, quindi modificare il messaggio visualizzato nella metà inferiore della scheda. Ogni voce è associata a un messaggio diverso, anche se per impostazione predefinita sono tutti e tre identici.

Invia messaggio di notifica per allegato con restrizioni a...
Quando viene recapitato un messaggio con un allegato corrispondente a una voce con restrizioni (elencate nella scheda Allegati), viene inviato un messaggio di avviso ai soggetti specificati in questa sezione. È possibile inviare un messaggio personalizzato al mittente, al destinatario e agli amministratori specificati nella scheda Destinatari. Per personalizzare il messaggio per una qualsiasi di queste tre voci, selezionarne una dall'elenco, quindi modificare il messaggio visualizzato nella metà inferiore della scheda. Ogni voce è associata a un messaggio diverso, anche se

per impostazione predefinita sono tutti e tre identici.

Oggetto messaggio:
Questo testo verrà visualizzato nell'intestazione "Subject:" del messaggio di notifica inviato.

Messaggio
Si tratta del messaggio che verrà inviato alla voce selezionata nell'elenco descritto in precedenza, purché la casella di controllo corrispondente sia selezionata. Il messaggio può essere modificato direttamente nella casella in cui viene visualizzato.

I file effettivi contenenti questo testo si trovano nella directory `MDaemon\app\`. Questi sono:

`cfattrem[adm].dat` – Messaggio per allegati con restrizioni - Amministratori
`cfattrem[rec].dat` – Messaggio per allegato con restrizioni - Destinatario
`cfattrem[snd].dat` – Messaggio per allegato con restrizioni - Mittente
`cfvirfnd[adm].dat` – Messaggio per rilevamento virus - Amministratori
`cfvirfnd[rec].dat` – Messaggio per rilevamento virus - Destinatario
`cfvirfnd[snd].dat` – Messaggio per rilevamento virus - Mittente

Per ripristinare l'aspetto originale di uno di questi messaggi, è sufficiente eliminare il file desiderato perché MDaemon lo crei nuovamente nello stato predefinito.

5.1.1.3.1 Macro per i messaggi

Nei messaggi di notifica e in altri messaggi generati da Filtro contenuti è possibile utilizzare alcune macro. È possibile utilizzare le macro:

`$ACTUALTO$`	Alcuni messaggi possono contenere un campo "ActualTo" che, generalmente, rappresenta la casella postale e l'host di destinazione immessi dall'utente originale prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
`$AV_VERSION$`	Indica la versione di SecurityPlus per MDaemon in uso.
`$CURRENTTIME$`	Questa macro viene sostituita con l'ora corrente in cui il messaggio viene elaborato.

`$ACTUALFROM$` Alcuni messaggi possono contenere un campo "ActualFrom" che, generalmente, rappresenta la casella postale e l'host di origine prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.

`$FILTERRULENAME$` Questa macro viene sostituita dal nome della regola i cui criteri corrispondono al messaggio.

`$HEADER:XX$` Questa macro viene sostituita nel messaggio riformattato dal valore dell'intestazione "xx". Ad esempio, se nel messaggio originale è presente "`TO: gianni@esempio.com`", la macro `$HEADER:TO$` verrà espansa in "gianni@esempio.com". Se nel messaggio originale è presente "Subject: Questo è l'oggetto", la macro `$HEADER:SUBJECT$` verrà sostituita dal testo "Questo è l'oggetto".

`$HEADER:MESSAGE-ID$` Analogamente alla macro `$HEADER:XX$`, questa macro viene sostituita dal valore dell'intestazione `Message-ID`.

`$LIST_ATTACHMENTS_REMOVED$` Questa macro visualizza gli allegati rimossi dal messaggio.

`$LIST_VIRUSES_FOUND$` Questa macro visualizza i virus rilevati in un messaggio.

`$MESSAGEFILENAME$` Questa macro restituisce il nome file del messaggio in corso di elaborazione.

`$MESSAGEID$` Simile alla macro `$HEADER:MESSAGE-ID$` precedente, a eccezione del fatto che rimuove i caratteri "<>" dal valore di message ID.

`$PRIMARYDOMAIN$` Restituisce il nome del dominio predefinito di MDaemon, specificato nella finestra di dialogo di configurazione del dominio predefinito (Impostazioni →Dominio predefinito/server).

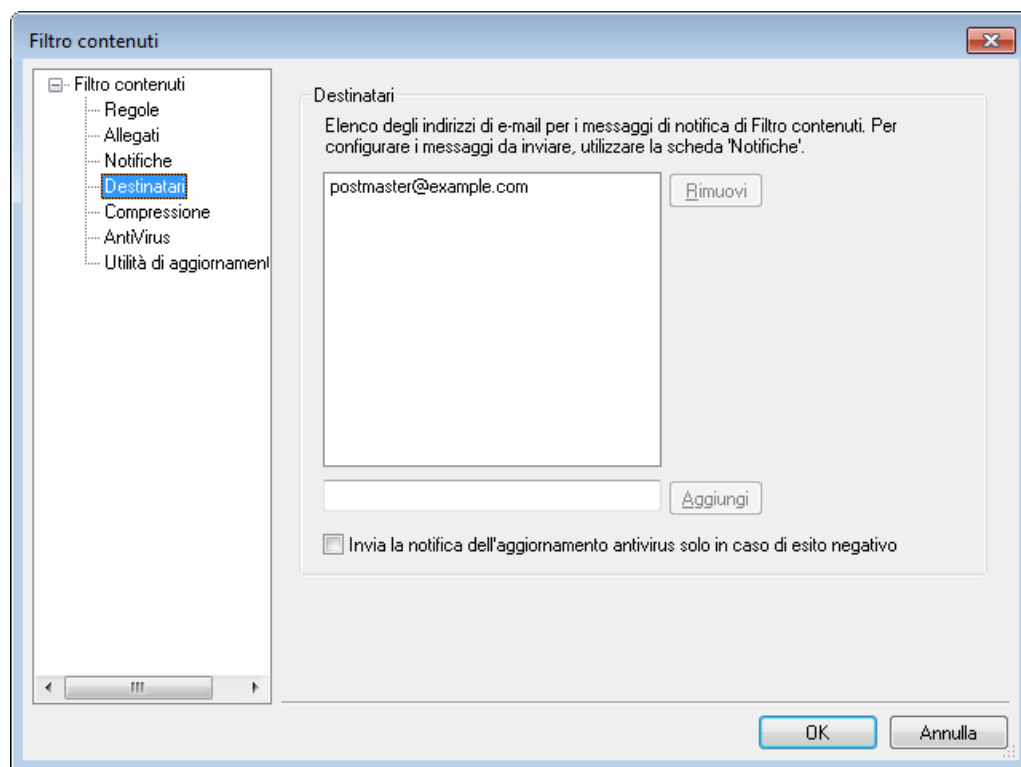
`$PRIMARYIP$` Questa macro restituisce l'indirizzo IP del dominio predefinito specificato nella finestra di dialogo di configurazione del dominio predefinito.

`$RECIPIENT$` Questa macro viene sostituita dall'indirizzo completo del destinatario del messaggio.

`$RECIPIENTDOMAIN$` Questa macro viene sostituita dal nome dominio del destinatario del messaggio.

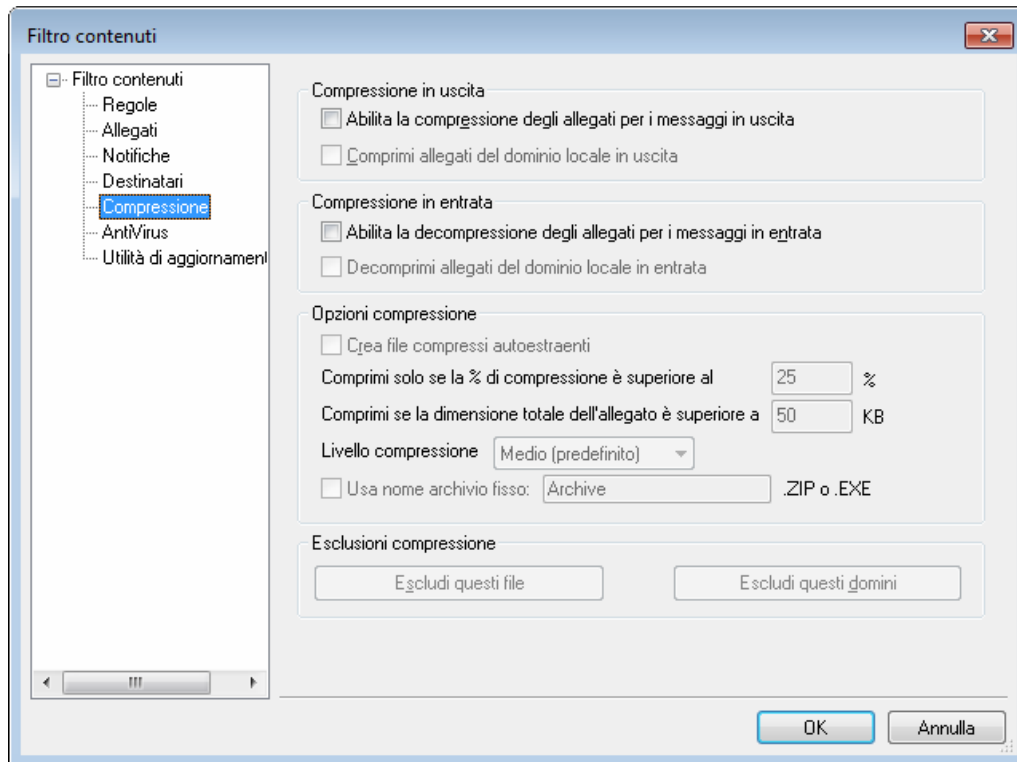
`$RECIPIENTMAILBOX$` Questa macro viene sostituita dalla casella postale del destinatario, ossia dal valore a sinistra di "@" nell'indirizzo e-mail.

`$REPLYTO$`	Questa macro restituisce il valore dell'intestazione "Reply-to" del messaggio.
`$SENDER$`	Questa macro restituisce l'indirizzo completo da cui è stato inviato il messaggio.
`$SENDERDOMAIN$`	Questa macro viene sostituita dal nome dominio del mittente del messaggio, ossia dal valore a destra di "@" nell'indirizzo e-mail.
`$SENDERMAILBOX$`	Questa macro viene sostituita dalla casella postale del mittente, ossia dal valore a sinistra di "@" nell'indirizzo e-mail.
`$SUBJECT$`	Questa macro viene sostituita dal testo contenuto nell'oggetto del messaggio.

5.1.1.4 Destinatari

Destinatari

Questo elenco di destinatari corrisponde alle diverse opzioni della scheda Notifiche utilizzate per inviare messaggi agli amministratori. Sono gli indirizzi ai quali viene inviato un messaggio di notifica quando viene selezionata un'opzione di tipo amministrativo della scheda Notifiche. Per aggiungere un indirizzo in questa sezione, digitarlo nell'apposita casella e fare clic su *Aggiungi*. Per rimuovere un indirizzo, selezionarlo dall'elenco e fare clic su *Rimuovi*.

Invia la notifica dell'aggiornamento antivirus solo in caso di esito negativo
Selezionare questa casella di controllo per inviare un messaggio di notifica solo se l'aggiornamento ha esito negativo.

5.1.1.5 Compressione

I comandi di questa scheda consentono di comprimere o decomprimere automaticamente gli allegati prima della consegna del messaggio. È possibile controllare il livello di compressione, nonché altri parametri e criteri di esclusione. Questa funzione può ridurre sensibilmente la larghezza di banda e il throughput necessari per consegnare i messaggi in uscita.

Compressione in uscita

Abilita la compressione degli allegati per i messaggi in uscita
Scegliere questa casella di controllo per abilitare la compressione automatica degli allegati dei messaggi remoti in uscita. Selezionando questo comando non verranno compressi tutti gli allegati, ma si attiverà semplicemente la funzione. Per determinare la compressione dei file è necessario specificare le altre impostazioni delle scheda.

Comprimi allegati del dominio locale in uscita
Specificare questo comando per applicare le impostazioni di compressione a tutta la posta in uscita, compresi i messaggi destinati a un altro indirizzo locale.

Compressione in entrata

Abilita la decompressione degli allegati per i messaggi in entrata
Selezionare questa casella di controllo per attivare la decompressione automatica degli allegati dei messaggi di posta remota in entrata. Quando viene recapitato un messaggio con un allegato compresso, quest'ultimo verrà decompresso prima che il messaggio venga consegnato nella casella postale dell'utente locale.

Decomprimi allegati del dominio locale in entrata
Selezionare questa casella di controllo per applicare la funzione di decompressione automatica anche agli allegati della posta locale.

Opzioni compressione

Crea file compressi autoestraenti
Fare clic su questa casella di controllo per abbinare alla compressione la creazione di file zip a estrazione automatica con estensione `EXE`. L'opzione si rivela utile quando i destinatari non dispongono di un'utilità di decompressione. I file autoestraenti possono essere decompressi facendo doppio clic sull'icona del file.

Comprimi solo se la % di compressione è superiore al XX%
MDaemon comprimerà l'allegato di un messaggio prima di inviarlo solo se la percentuale di compressione supera il valore specificato in questo campo. Se ad esempio il valore specificato è 20 e la percentuale di compressione di un determinato allegato non raggiunge il 21%, questo non verrà compresso prima dell'invio.

Per determinarne la percentuale di compressione, un file deve essere innanzitutto compresso. Pertanto, la funzione non impedisce che i file vengano compressi, ma consente solo di evitare che vengano inviati allegati in formato compresso quando la relativa percentuale di compressione non raggiunge il valore specificato. In altri termini, se i file non possono essere compressi più del valore specificato, la compressione non verrà eseguita e il messaggio verrà inviato con gli allegati invariati.

Comprimi se la dimensione totale dell'allegato è superiore a XX KB
Se la funzione di compressione automatica dell'allegato è abilitata, verranno compressi solo gli allegati con dimensione complessiva superiore al valore specificato in questo campo. I messaggi associati ad allegati con dimensione inferiore a questa soglia vengono di norma consegnati senza alcuna modifica degli allegati.

Livello compressione
In questa casella di riepilogo a discesa è possibile scegliere il livello di compressione da applicare agli allegati compressi automaticamente. Sono disponibili tre livelli di compressione: minimo (compressione più rapida ma limitata), medio (valore predefinito) e massimo (compressione meno rapida ma più efficiente).

Usa nome archivio fisso: [nome archivio]
Se si desidera che agli allegati compressi automaticamente corrisponda uno specifico

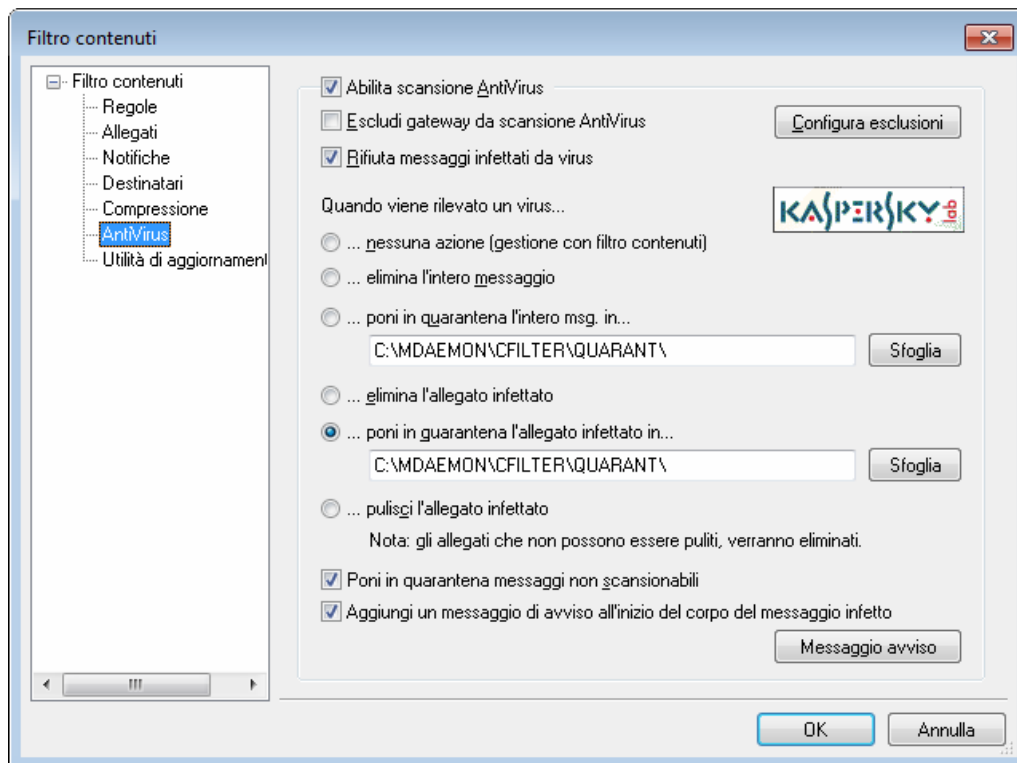
nome file, selezionare questa casella di controllo e scegliere il nome.

Esclusioni compressione

Escludi questi file
Fare clic sul pulsante fornito per specificare i file da escludere dalle funzioni di compressione automatica. Se l'allegato di un messaggio corrisponde a uno di questi nomi file, la compressione non verrà applicata, indipendentemente dalle impostazioni specificate. I caratteri jolly sono consentiti nelle voci dell'elenco. Ad esempio, se si specifica "*.exe", i file con estensione "exe" non verranno compressi.

Escludi questi domini
Fare clic sul pulsante fornito per specificare i domini dei destinatari i cui messaggi devono essere esclusi dalla compressione automatica. Gli allegati dei messaggi associati a questi domini non verranno compressi, indipendentemente dalle impostazioni specificate.

5.1.2 AntiVirus

5.1.2.1 AntiVirus

Questa scheda e quella dell'utilità di aggiornamento AntiVirus 235 risultano disponibili solo se SecurityPlus per MDaemon è installato. Per ottenere SecurityPlus per MDaemon, visitare il sito www.altn.com.

Configurazione scansione

Abilita scansione AntiVirus
Selezionare questa casella di controllo per abilitare la scansione antivirus dei messaggi. Alla ricezione di un messaggio contenente allegati, SecurityPlus per MDaemon si attiverà ed eseguirà la scansione degli allegati prima che il messaggio venga consegnato alla destinazione finale.

Escludi gateway dalla scansione antivirus
Selezionare questa casella di controllo per escludere dalla scansione antivirus i messaggi associati a uno o più gateway di dominio di MDaemon. L'opzione è utile se si preferisce delegare la scansione di questi messaggi al server di posta del dominio. Per ulteriori informazioni sui gateway di dominio, vedere Gateway di dominio 458.

Rifiuta messaggi infettati da virus
Selezionare questa casella di controllo per eseguire la scansione antivirus durante la sessione SMTP anziché al suo completamento e rifiutare i messaggi infettati. Poiché ogni messaggio in entrata viene analizzato prima che MDaemon lo accetti ufficialmente e termini la sessione, per il messaggio, che a livello tecnico non è stato ancora consegnato, risponde il server di invio. Il messaggio può essere rifiutato non appena viene rilevato un virus. In caso di rifiuto, non verrà intrapresa alcuna delle azioni specificate in questa finestra di dialogo. Non sarà eseguita la procedura di pulitura o quarantena, né verranno inviati messaggi di notifica. Questo comportamento consente di ridurre la diffusione di messaggi infettati e di notifica di virus.

Il file registro SMTP include i risultati dell'elaborazione AntiVirus. È possibile visualizzare i risultati seguenti:

- Il messaggio è stato analizzato ed è stata rivelata la presenza di un virus.
- Il messaggio è stato analizzato e non è stato rilevato alcun virus.
- Non è stato possibile analizzare il messaggio (solitamente perché è impossibile accedere o aprire un allegato in formato ZIP o di altro tipo).
- Non è stato possibile eseguire la scansione del messaggio (supera il limite di dimensione massima).
- Si è verificato un errore durante la scansione.

Configura esclusioni
Fare clic sul pulsante Configura esclusioni per specificare gli indirizzi dei destinatari da escludere dalla scansione antivirus. SecurityPlus per MDaemon non esegue la scansione dei messaggi associati a questi indirizzi. È consentito utilizzare i caratteri jolly negli indirizzi. La funzione può pertanto essere utilizzata per escludere interi domini o determinate caselle postali di qualsiasi dominio, ad esempio "*@esempio.com" o "ArchivioVirus@*".

Quando viene rilevato un virus
Selezionare una delle opzioni di questa sezione per specificare l'azione da eseguire quando SecurityPlus per MDaemon rileva un virus.

Nessuna azione (gestione con filtro contenuti)
Scegliere questa opzione se nessuna delle azioni descritte in precedenza deve essere eseguita e si preferisce impostare le regole di Filtro contenuti per specificare una soluzione alternativa.

Elimina l'intero messaggio
Specificando questa opzione, verrà eliminato l'intero messaggio anziché il solo allegato. Poiché viene eliminato l'intero messaggio, l'opzione "*Aggiungi un messaggio di avviso...*" non è applicabile. È comunque possibile inviare una notifica al destinatario utilizzando i comandi della scheda Notifiche.

Poni in quarantena l'intero msg. in
Questa opzione è simile all'opzione "*Elimina l'intero messaggio*" descritta in precedenza, ma in questo caso il messaggio viene posto in quarantena nella posizione specificata e non viene eliminato.

Elimina l'allegato infettato
Scegliendo questa opzione, l'allegato infettato verrà eliminato. Il messaggio viene comunque consegnato al destinatario, ma senza l'allegato infettato. Il comando "*Aggiungi un messaggio di avviso*", visualizzato nella parte inferiore della finestra di dialogo, consente di aggiungere un testo al messaggio per segnalare all'utente l'eliminazione di un allegato infettato.

Poni in quarantena l'allegato infettato in
Questa opzione consente di specificare una posizione in cui porre in quarantena gli allegati infettati, in alternativa all'eliminazione o alla pulizia. Analogamente all'opzione "*Elimina l'allegato infettato*", il messaggio viene consegnato al destinatario senza l'allegato.

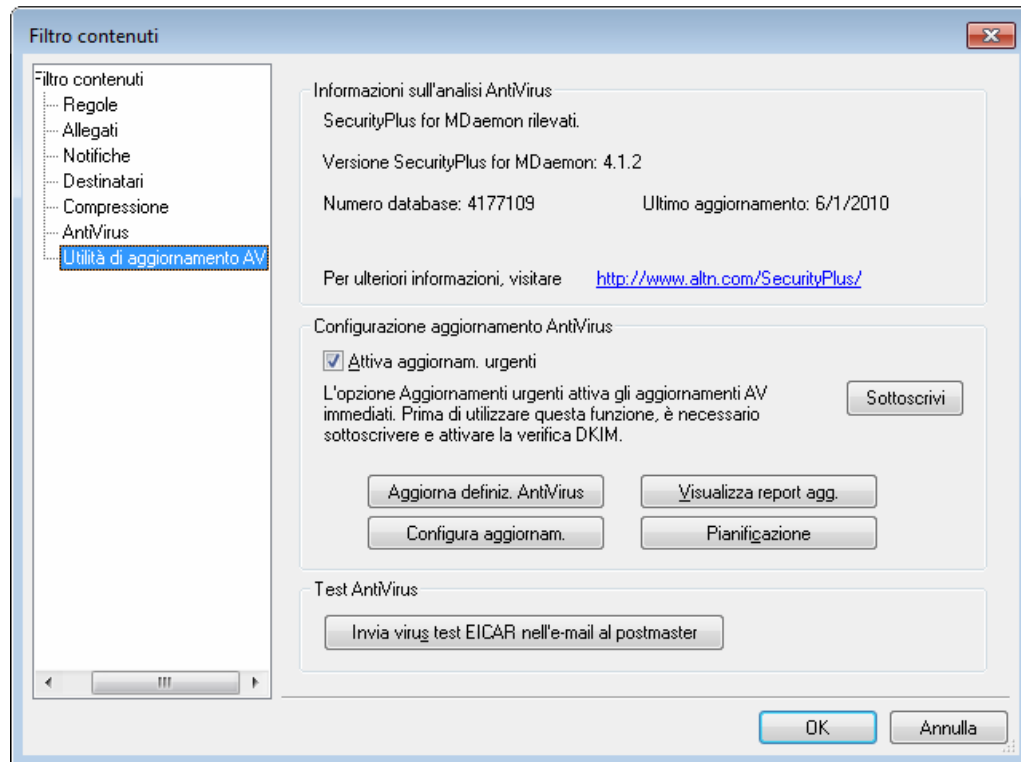
Elimina l'allegato infettato
Se si seleziona questa opzione, SecurityPlus per MDaemon tenterà di pulire l'allegato, disattivando il virus che lo ha infettato. Se l'allegato non può essere pulito, verrà eliminato.

Aggiungi un messaggio di avviso all'inizio del corpo del messaggio infetto
Se è selezionata una delle opzioni illustrate in precedenza, è possibile specificare questa casella di controllo per aggiungere un testo di avviso all'inizio del messaggio associato all'allegato infettato prima di consegnarlo al destinatario. In questo modo, è possibile notificare al destinatario l'eliminazione dell'allegato e indicarne il motivo.

Messaggio avviso
Fare clic su questo pulsante per visualizzare il testo di avviso da aggiungere ai messaggi quando si utilizza la funzione corrispondente. Una volta apportate le modifiche al testo, fare clic su "OK" per chiudere la finestra di dialogo e salvare le modifiche.

Per ulteriori informazioni, vedere:

Utilità di aggiornamento AntiVirus 235
Filtro contenuti e SecurityPlus 211

5.1.2.2 Utilità di aggiornamento AntiVirus

I comandi di questa scheda consentono di aggiornare in modo manuale o automatico le definizioni dei virus di SecurityPlus per MDaemon. Le funzioni disponibili includono un'utilità di aggiornamento automatico, un visualizzatore di report per il monitoraggio dello scaricamento degli aggiornamenti e un'utilità che consente di verificare il corretto funzionamento della scansione antivirus.

Informazioni sull'analisi AntiVirus

In questa sezione viene indicato se SecurityPlus per MDaemon è installato e vengono fornite informazioni sulla versione eventualmente in esecuzione. È inoltre riportata la data dell'ultimo aggiornamento delle definizioni dei virus.

Configurazione aggiornamento AntiVirus

Attiva aggiornamenti urgenti
Selezionare questa casella di controllo per attivare gli aggiornamenti urgenti. Se questa funzione è abilitata, SecurityPlus per MDaemon si connette e scarica l'aggiornamento con priorità elevata non appena viene ricevuto un messaggio che segnala un aggiornamento urgente. Per ricevere questi messaggi, è necessario

essere iscritti alla funzionalità "Aggiornamenti urgenti". Vedere l'opzione *Sottoscrivi* descritta di seguito.

Sottoscrivi
Facendo clic su questo pulsante, il browser predefinito apre la pagina per l'iscrizione alla lista Urgent Updates (Aggiornamenti urgenti) del sito di Alt-N Technologies. In questa pagina, immettere il nome dominio da aggiungere alla lista di distribuzione relativa agli aggiornamenti urgenti. Quando è disponibile un aggiornamento urgente delle definizioni dei virus di SecurityPlus per MDaemon, al dominio viene inviato un apposito messaggio. SecurityPlus per MDaemon viene aggiornato non appena si riceve il messaggio.

Aggiorna definizioni AntiVirus
Fare clic su questo pulsante per eseguire l'aggiornamento manuale delle definizioni dei virus. L'utilità di aggiornamento si connetterà immediatamente.

Configura aggiornamenti
Fare clic su questo pulsante per aprire la finestra di dialogo Configurazione utilità di aggiornamento Security Plus per MDaemon237. Nella finestra di dialogo sono presenti quattro schede: URL aggiornamento, Connessione, Proxy e Varie.

Visualizza report aggiornamento
Il pulsante *Visualizza report aggiornamento* consente di aprire la finestra di visualizzazione del registro di SecurityPlus in cui sono elencati gli orari, le azioni eseguite e altre informazioni relative a ogni aggiornamento.

Pianificazione
Questo pulsante consente di aprire Pianificazione eventi attivando la scheda Aggiornamenti AntiVirus163, utilizzata per pianificare le verifiche di disponibilità di aggiornamenti delle definizioni dei virus in giorni e orari specifici o in base a intervalli regolari. In questa scheda è inoltre disponibile l'opzione *Attiva aggiornamenti urgenti* che consente di attivare o disattivare gli aggiornamenti urgenti automatici. L'opzione ha la stessa funzionalità dell'omonimo comando descritto in precedenza.

Test AntiVirus

Invia virus test EICAR nell'e-mail al postmaster
Fare clic su questo pulsante per inviare al postmaster un messaggio di testo infettato con EICAR. Si tratta di un allegato innocuo, utilizzato per collaudare SecurityPlus per MDaemon. Per controllare il comportamento di MDaemon alla ricezione del messaggio, osservare la finestra del registro di Filtro contenuti nell'interfaccia principale di MDaemon. A seconda delle impostazioni, le righe del registro possono essere le seguenti:

```
Mon 25.02.08 18:14:49: Processing C:\MDAEMON\LOCALQ\md75000001128.msg
Mon 25.02.08 18:14:49: > eicar.com (C:
\MDaemon\CFilter\TEMP\cf1772420862.att)
Mon 25.02.08 18:14:49: > Message from: postmaster@mycompany.com
Mon 25.02.08 18:14:49: > Message to: postmaster@mycompany.com
Mon 25.02.08 18:14:49: > Message subject: EICAR Test Message
Mon 25.02.08 18:14:49: > Message ID: <MDAEMON10001200202251814.
AA1447619@mycompany.com>
```

```
Mon 25.02.08 18:14:49: Performing viral scan...
Mon 25.02.08 18:14:50: > eicar.com is infected by EICAR-Test-File
Mon 25.02.08 18:14:50: > eicar.com was removed from message
Mon 25.02.08 18:14:50: > eicar.com quarantined to C:
\MDAEMON\CFILTER\QUARANT\
Mon 25.02.08 18:14:50: > Total attachments scanned : 1 (including
multipart/alternatives)
Mon 25.02.08 18:14:50: > Total attachments infected : 1
Mon 25.02.08 18:14:50: > Total attachments disinfected: 0
Mon 25.02.08 18:14:50: > Total attachments removed : 1
Mon 25.02.08 18:14:50: > Total errors while scanning : 0
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@mycompany.com (sender)
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@mycompany.com (recipient)
Mon 25.02.08 18:14:50: > Virus notification sent to
postmaster@mycompany.com (admin)
Mon 25.02.08 18:14:50: > Virus notification sent to postmaster@example.
com (admin)
Mon 25.02.02 18:14:50: Processing complete (matched 0 of 12 active
rules)
```

Per ulteriori informazioni, vedere:

Finestra di dialogo Configurazione aggiornamento AntiVirus 237
AntiVirus 232
Filtro contenuti e SecurityPlus 211

5.1.2.2.1 Finestra di dialogo Configurazione aggiornamento AntiVirus

Il pulsante *Configura aggiornamenti* della scheda AV Updater 235 consente di aprire la finestra di dialogo Updater Configuration. Comprende le quattro schede seguenti:

Aggiorna URL
La scheda URL aggiornamento consente di indicare i server in cui SecurityPlus per MDaemon può cercare gli aggiornamenti. È possibile lasciare che gli URL vengano gestiti automaticamente da SecurityPlus oppure immetterli manualmente.

Connessione
Questa scheda consente di specificare il profilo di connessione a Internet da utilizzare per la connessione ai siti di aggiornamento. Se si specifica l'opzione "*Utilizza la configurazione Internet specificata nel Pannello di controllo*", verranno utilizzate le impostazioni Internet predefinite. L'opzione "*Configura manualmente la connessione a Internet*" e i controlli utente successivi possono essere utilizzati per selezionare manualmente un profilo di connessione e per definire le impostazioni relative a nome utente e password.

Proxy
Nella scheda Proxy sono presenti le opzioni che consentono di specificare le impostazioni del server HTTP o FTP necessarie alla configurazione di rete corrente

per la connessione ai siti di aggiornamento.

Varie
Le opzioni della scheda Varie consentono di configurare la registrazione delle attività dell'utilità di aggiornamento, specificando se registrare tali attività in un file e indicando la dimensione massima di quest'ultimo.

Per ulteriori informazioni, vedere:

Utilità di aggiornamento AntiVirus 235
AntiVirus 232
Filtro contenuti e SecurityPlus 211

5.2 Protezione attacchi

Protezione attacchi (Outbreak Protection, OP) è una rivoluzionaria tecnologia antispam, antivirus e antiphishing che consente di proteggere automaticamente e in tempo reale una infrastruttura di posta elettronica MDaemon entro pochissimi minuti dall'inizio di un attacco. La funzione Protezione attacchi, integrata in SecurityPlus per MDaemon, richiede la versione 3.0 di SecurityPlus per MDaemon o una versione successiva e la versione 9.5 di MDaemon PRO o una versione successiva. Per accedere a tale funzione, selezionare Sicurezza » Protezione attacchi oppure premere CTRL+MAIUSC+1.

La funzione Protezione attacchi è completamente indipendente dal contenuto, ossia non dipende dall'analisi lessicale del contenuto del messaggio e non richiede quindi regole euristiche, funzioni di filtro dei contenuti o aggiornamenti delle definizioni antivirus. Grazie a questa caratteristica, la funzione di protezione non viene disattivata dall'aggiunta di testo spurio, da astute modifiche ortografiche, da tattiche di ingegneria sociale, da ostacoli linguistici o da differenze di codifica. Protezione attacchi, al contrario, si basa sull'analisi matematica della struttura dei messaggi e sulle caratteristiche di distribuzione mediante SMTP. La funzione analizza i "modelli" associati alla trasmissione delle e-mail e li confronta con i modelli raccolti da milioni di messaggi di posta trasmessi in tutto il mondo. L'analisi e il confronto vengono eseguiti in tempo reale.

Poiché i messaggi vengono analizzati in tutto il mondo e in tempo reale, la protezione è disponibile in pochi minuti, spesso entro pochi secondi dall'inizio dell'attacco. Nel caso dei virus, questo livello di protezione è fondamentale perché la verifica e la pubblicazione di un aggiornamento delle definizioni virus a seguito di un nuovo attacco possono richiedere diverse ore e può trascorrere un tempo ancora superiore prima che l'aggiornamento venga installato. Durante questo periodo di tempo, i server privi di Protezione attacchi sono vulnerabili al nuovo attacco. Analogamente, è necessario molto tempo anche per l'analisi di un nuovo messaggio spam e per la creazione di un'apposita regola di filtro che ne consentano l'individuazione da parte dei tradizionali sistemi euristici o basati sul contenuto.

È opportuno tenere presente, tuttavia, che la funzione Protezione attacchi di SecurityPlus non rappresenta un'alternativa alle tradizionali tecniche antivirus, antispam e antiphishing. Questa tecnologia offre un ulteriore livello di protezione che si aggiunge agli strumenti basati su algoritmi euristici, su file di definizione dei virus o sul contenuto

disponibili in SecurityPlus e in MDaemon. Protezione attacchi è una funzione specificamente progettata per fronteggiare attacchi su vasta scala anziché singoli o specifici messaggi infetti da virus o malware già noto che vengono gestiti più efficacemente dagli strumenti tradizionali.

Protezione attacchi si basa sulla tecnologia CommTouch RPD e Zero-Hour. che opera estraendo modelli dalla posta in arrivo e confrontandoli con i modelli recuperati grazie all'analisi di milioni di messaggi e-mail su Internet da numerosi origini sparse in tutto il mondo. Il contenuto effettivo dei messaggi non viene mai trasmesso, né può essere derivato dai modelli estratti.

Per ulteriori informazioni su SecurityPlus e su Protezione attacchi, consultare la parte rimanente di questa sezione o visitare il sito: www.altn.com.

Protezione attacchi

Protezione attacchi (OP, Outbreak Protection) è un sistema in tempo reale in grado di individuare e bloccare entro pochi minuti gli attacchi condotti mediante virus, messaggi spam e determinati contenuti offensivi e illegali.

☑ Abilita Protezione attacchi

I virus devono essere ◉ bloccati in tempo reale ○ posti in quarantena

I messaggi vengono collocati nella cartella di quarantena SecurityPlus.

I messaggi spam devono essere ◉ bloccati in tempo reale ○ accettati poi filtrati Punteggio 2.5

I contenuti offensivi e illegali (IWF) devono essere ◉ bloccati in tempo reale ○ accettati poi filtrati Punteggio 2.5

☐ Con il blocco della posta indesiderata, blocca anche i messaggi indesiderati collettivi

☑ Chiudi sessioni di posta una volta bloccati virus, spam o messaggio IWF

☑ Registra attività elaborazione in file registro plug-in

Eccezioni

☑ Escludi da elaborazione le sessioni SMTP autenticate

☑ Escludi da elaborazione le sessioni SMTP da IP accreditati

☑ La posta elettronica approvata SPF/ID mittente/DK/DKIM è esente dall'elaborazione OP

☑ Escludi da elaborazione gli indirizzi nelle liste bianche di Spam Trap e Spam Filter

La lista bianca utilizza i valori della busta, non i valori dell'intestazione del messaggio.

Falsi positivi e falsi negativi

I processi di rilevamento e classificazione sono in continua evoluzione.

Per lo spam, è possibile segnalare falsi positivi a spamfp@altn.com e falsi negativi a spamfn@altn.com. Per i virus, è possibile falsi positivi a virusfp@altn.com e falsi negativi a virusfn@altn.com.

Inviare i messaggi originali come allegati MIME. Non inoltrare i messaggi per evitare di perdere informazioni importanti dell'intestazione.

OK Annulla

Protezione attacchi

Abilita Protezione attacchi

Fare clic su questa casella di controllo per abilitare Protezione attacchi nel server in

uso. I messaggi in entrata verranno analizzati per verificare se sono relativi ad attacchi in corso di tipo virale, spam o phishing. Le rimanenti opzioni presenti nella scheda di dialogo consentono di definire il destino dei messaggi che rappresentano un attacco e di indicare i mittenti che vengono esclusi dall'elaborazione OP.

I virus devono essere...

bloccati in tempo reale
Selezionare questa opzione se si desidera bloccare durante l'elaborazione SMTP i messaggi che rappresentano un attacco di tipo virale. Questi messaggi non verranno posti in quarantena né recapitati ai destinatari previsti, ma verranno respinti direttamente dal server.

posti in quarantena
Selezionare questa opzione se si desidera accettare i messaggi che rappresentano un attacco di tipo virale. I messaggi non verranno respinti dal server, ma verranno posti in quarantena anziché essere recapitati ai destinatari previsti. I messaggi vengono collocati nella cartella di quarantena di SecurityPlus.

I messaggi spam devono essere...

bloccati in tempo reale
Selezionare questa opzione se si desidera bloccare durante l'elaborazione SMTP i messaggi che rappresentano un attacco di tipo spam. Questi messaggi non verranno contrassegnati come spam né recapitati ai destinatari previsti, ma verranno respinti direttamente dal server. I messaggi classificati da Protezione attacchi come posta collettiva o "bulk" non vengono bloccati da questa opzione, a meno che si attivi l'opzione *Con il blocco della posta indesiderata, blocca anche i messaggi indesiderati collettivi*. È possibile che i messaggi classificati come collettivi da OP siano parte di liste di distribuzione di grandi dimensioni o di altri contenuti ampiamente distribuiti; di conseguenza possono essere considerati o meno spam. Per questo motivo, non è consigliabile bloccare o assegnare un punteggio in senso negativo a questo tipo di messaggi mediante Protezione attacchi.

accettati poi filtrati
Selezionare questa opzione se si desidera accettare i messaggi che rappresentano un attacco di tipo spam, in modo da sottoporli alla successiva elaborazione di Spam filter e di Filtro contenuti. Questi messaggi non vengono bloccati da Protezione attacchi, ma il relativo punteggio spam viene corretto in base all'opzione *Punteggio*.

Se si utilizza l'opzione *accettati poi filtrati*, Protezione attacchi non blocca direttamente i messaggi spam. Questi ultimi, tuttavia, possono essere bloccati da MDaemon durante l'elaborazione SMTP se Spam Filter utilizza l'opzione *SMTP rifiuta i msg con punteggi superiori o uguali a [xx]* della schermata Spam Filter 244.

Se ad esempio l'opzione relativa al punteggio determina un punteggio Spam Filter pari a 15.0 per un messaggio,

> quest'ultimo viene comunque rifiutato come spam se l'opzione di Spam Filter "*SMTP rifiuta....*" prevede lo scarto dei messaggi con un punteggio pari o superiore a 15.0.

Punteggio
Se si utilizza l'opzione *accettati poi filtrati*, questo è il valore aggiunto al punteggio spam del messaggio assegnato da Spam Filter qualora Protezione attacchi accerti che il messaggio rappresenta un attacco spam.

Contenuti IWF

L'opzione seguente viene applicata ai contenuti segnalati dall'IWF (Internet Watch Foundation) perché associati a siti contenenti immagini di abusi sui bambini, ossia pedopornografiche. L'opzione consente di uilizzare un elenco di URL forniti dall'IWF per individuare e contrassegnare i messaggi che si riferiscono a tali contenuti. La fondazione IWF opera come servizio Internet indipendente per la segnalazione di contenuto potenzialmente illegale, incluse le immagini relative a pedopornografia o ad abusi compiuti sui bambini, in qualsiasi parte del mondo. La fondazione opera in coordinamento con le forze dell'ordine, con i governi, con l'industria Internet nel suo complesso e con il pubblico per contrastare la disponibilità online di contenuto illegale. L'elenco di URL fornito dalla fondazione viene aggiornato quotidianamente con i nuovi siti che ospitano immagini relative ad abusi sui bambini.

Molte organizzazioni hanno definito regole di conformità interne che governano il contenuto dei messaggi e-mail inviati o ricevuti dai propri impiegati, in particolare per quanto riguarda il materiale illegale o pornografico. Molte nazioni, inoltre, hanno proibito per legge l'invio o la ricezione di tale contenuto. Questa funzionalità può semplificare la conformità a queste disposizioni.

Per ulteriori informazioni sulla fondazione IWF, vedere:

http://www.iwf.org.uk/

I contenuti offensivi e illegali (IWF) devono essere...

bloccati in tempo reale
Scegliere questa opzione se si desidera rifiutare, durante l'elaborazione SMTP, i messaggi in entrata con contenuto segnalato dalla fondazione IWF.

accettati poi filtrati
Scegliere questa opzione se si desidera aumentare il punteggio spam di un messaggio con contenuto segnalato dalla fondazione IWF anziché respingerlo. Il punteggio spam del messaggio viene aumentato del valore specificato nel campo *Punteggio*.

Punteggio
Se si utilizza l'opzione *accettati poi filtrati*, questo è il valore aggiunto al punteggio spam del messaggio assegnato da Spam Filter qualora contenga contenuto segnalato dalla fondazione IWF.

Con il blocco della posta indesiderata, blocca anche i messaggi indesiderati collettivi
Protezione attacchi talvolta individua messaggi che possono essere considerati spam ma non sono inviati da botnet o da spammer noti, situazione comune nel caso di invio di posta collettiva (bulk) e di newsletter. Protezione attacchi classifica questi messaggi come "*Spam (bulk)*" anziché ""*Spam (confirmed)*". Selezionare questa opzione se si desidera applicare la funzionalità di blocco di Protezione attacchi anche alla posta classificata "*Spam (bulk)*". Se l'opzione è disabilitata, la funzionalità di blocco interessa solo i messaggi classificati come "*Spam (confirmed)*". La scelta di accettare questo tipo di spam per elaborarla in seguito può essere necessaria nel caso si desideri ricevere posta collettiva, ma non si possano inserire nella lista bianca i mittenti o i destinatari.

Registra attività elaborazione in file registro plug-in
Selezionare questa casella di controllo se si desidera registrare tutte le attività di Protezione attacchi nel file registro relativo ai plug-in di MDaemon.

Eccezioni

Escludi da elaborazione le sessioni SMTP autenticate
Se si abilita questa opzione, le sessioni SMTP autenticate vengono escluse dall'elaborazione di Protezione attacchi. In altre parole, i messaggi inviati durante tali sessioni non vengono verificati da Protezione attacchi.

Escludi da elaborazione le sessioni SMTP da IP accreditati
Abilitare questa opzione se si desidera escludere dall'elaborazione di Protezione attacchi gli indirizzi IP accreditati. In questo caso, i messaggi provenienti da un server al quale è associato un indirizzo IP accreditato non vengono sottoposti a verifica da Protezione attacchi.

La posta elettronica approvata SPF/ID mittente/DK/DKIM è esente dall'elaborazione OP
Selezionare questa casella di controllo se si desidera escludere dall'elaborazione di Protezione attacchi i messaggi il cui dominio mittente sia incluso nell'elenco approvato 303 e venga convalidato da SPF, ID mittente, DK o DKIM.

Gli indirizzi lista bianca di Spam Trap e Spam Filter vengono esclusi dall'elaborazione di Protezione attacchi
Questa opzione consente di escludere da Protezione attacchi le liste bianche di Honeypot spam 273 e di Spam Filter. L'elenco esclusioni viene applicato al destinatario, ossia al valore RCPT fornito durante la sessione SMTP. La lista bianca (per mittente) viene applicata al mittente, ossia al valore MAIL fornito durante la sessione SMTP. Queste operazioni non sono basate sui valori dell'intestazione del messaggio.

Falsi positivi e falsi negativi

I falsi positivi, ossia la classificazione come attacco di un messaggio in realtà legittimo, rappresentano un'eventualità estremamente rara. Qualora si verifichi una tale eventualità, tuttavia, è possibile inviare il messaggio falso positivo all'indirizzo **spamfp@altn.com** nel caso di spam o di phishing oppure all'indirizzo **virusfp@altn.com** nel caso di virus. Ciò consentirà di raffinare e perfezionare i processi di individuazione e classificazione di Protezione attacchi.

I falsi negativi, ossia la classificazione come legittimo di un messaggio che in realtà è spam o è associato a un attacco, rappresentano un'eventualità più frequente. È opportuno tenere presente che la funzione Protezione attacchi non è stata progettata per l'intercettazione di tutti gli attacchi di tipo spam, virus o simili. Questa funzione rappresenta un ulteriore livello di protezione specificamente rivolto agli attacchi. I messaggi meno recenti, quelli con un obiettivo specifico e simili che non fanno parte di un attacco in corso, potrebbero superare le verifiche eseguite da Protezione attacchi, ma verranno intercettati dalle altre funzioni di SecurityPlus per MDaemon che rientrano nelle fasi di elaborazione successive. Qualora si verifichi un falso negativo, tuttavia, è possibile inviare il messaggio in questione all'indirizzo **spamfn@altn.com** nel caso di spam o di phishing oppure all'indirizzo **virusfn@altn.com** nel caso di virus. Ciò consentirà di raffinare e perfezionare i processi di individuazione e classificazione di Protezione attacchi.

Qualora si desideri inviare un messaggio classificato in modo inappropriato, non inoltrare il messaggio e-mail originale ma inviarlo sotto forma di allegato MIME. In caso contrario, le intestazioni e altre informazioni fondamentali ai fini della classificazione verrebbero perse.

5.3 Spam Filter

5.3.1 Spam Filter

Spam Filter è una delle principali funzionalità della vasta gamma di strumenti per la prevenzione dello spam disponibile in MDaemon. Spam Filter incorpora una logica di elaborazione euristica che esamina i messaggi e-mail in arrivo calcolando un "punteggio" basato su un sistema complesso di regole. Questo punteggio viene utilizzato per determinare la probabilità che un messaggio sia di tipo spam e per intraprendere alcune operazioni come, ad esempio, rifiutare un messaggio, contrassegnarlo come possibile spam e così via.

Gli indirizzi possono essere inseriti in liste bianche o in liste nere oppure esclusi da qualsiasi controllo di Spam Filter. È possibile includere nei messaggi un report spam che mostra i punteggi di spam e la modalità con cui sono stati calcolati, oppure creare un report in una e-mail distinta che contiene in allegato il messaggio spam originale. Inoltre, è possibile utilizzare anche l'apprendimento bayesiano 247 per consentire a Spam Filter di incrementare con il tempo l'efficacia di identificazione dello spam aumentando, così, la sua affidabilità.

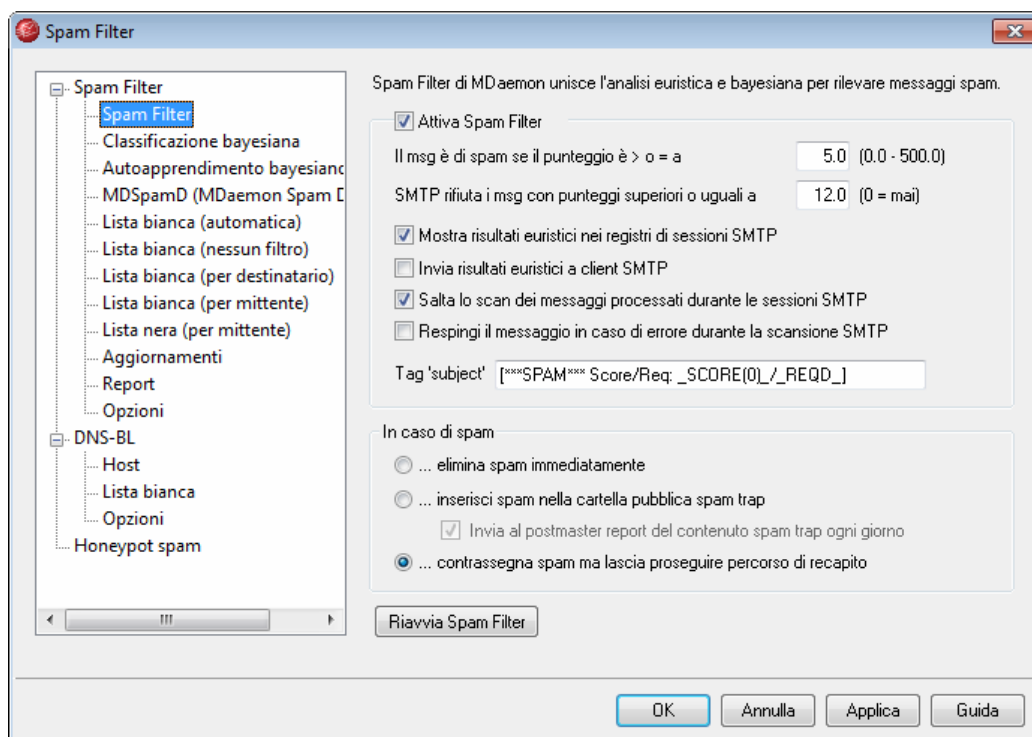
Infine, dopo aver esaminato diverse migliaia di messaggi spam, le regole sono state ottimizzate con il tempo diventando sempre più affidabili nel rilevare messaggi spam. Tuttavia, per soddisfare ogni specifica esigenza, è possibile personalizzare o aggiungere nuove regole modificando i file di configurazione di Spam Filter.

Spam Filter di MDaemon usa una tecnologia open-source integrata di tipo euristico molto diffusa. La home page del relativo progetto open-source è disponibile all'indirizzo

`http://www.spamassassin.org`

Per ulteriori informazioni, vedere:

Spam Filter 244
Liste nere DNS 267

5.3.1.1 Spam Filter

Attiva Spam Filter

Selezionare questa casella di controllo per attivare il sistema euristico per il filtro spam e il punteggio messaggi. Finché non viene abilitata questa opzione, non è disponibile alcuna delle opzioni Spam Filter della schermata.

Il msg è spam se il punteggio è > o = a XX (0,0-500,0)
Il valore specificato in questo campo indica la soglia di spam confrontata con i singoli punteggi di spam. Ogni messaggio con un punteggio maggiore o uguale a questo valore è considerato spam e determina, dunque, l'esecuzione delle operazioni previste in base alle impostazioni di Spam Filter.

SMTP rifiuta i msg con punteggi superiori o uguali a XX (0=mai)
Usare questa opzione per determinare una soglia di punteggio di spam, superata la quale i messaggi vengono respinti. Quando il punteggio è maggiore o uguale a questo valore, il messaggio viene respinto direttamente anziché procedere con le altre opzioni ed essere eventualmente consegnato. È opportuno che il valore di questa opzione sia sempre maggiore del valore che corrisponde all'opzione "*Il messaggio è spam se il punteggio è*" descritta in precedenza. In caso contrario, il messaggio non è

mai considerato spam, vengono applicate tutte le altre opzioni di Spam Filter e il messaggio viene respinto direttamente durante la consegna. Inserire in questo campo il valore "0" se si desidera disattivare l'analisi durante la sessione SMTP e respingere tutti i messaggi, ignorando i punteggi. Se la scansione SMTP è disattivata, sui messaggi accettati viene eseguita un'analisi basata sulle code. L'impostazione predefinita di questo campo è "12.0".

Esempio:

Se la soglia del punteggio di spam è impostata su 5.0 e quella affinché un messaggio venga respinto è impostata su 10.0, allora tutti i messaggi con un punteggio di spam maggiore o uguale a 5.0 ma inferiore a 10.0 vengono considerati spam e gestiti in base alle altre impostazioni di Spam Filter. Durante la consegna, ciascun messaggio con un punteggio di spam maggiore o uguale a 10.0 viene respinto.

È opportuno controllare le prestazioni di Spam filter nel tempo e, se necessario, modificare i valori delle soglie che consentono di considerare un messaggio spam o respingerlo. La maggior parte degli utenti, tuttavia, considera che la soglia del punteggio di spam impostata a 5.0 cattura più spam, con un numero relativamente basso di messaggi considerati erroneamente negativi, denominati anche "falsi negativi" (ovvero spam che non viene riconosciuto come tale), e raramente messaggi considerati erroneamente positivi, denominati anche "falsi positivi" (ovvero messaggi contrassegnati come spam ma che in realtà non lo sono). Una soglia di rifiuto impostata tra 10 e 15 fa sì che vengano respinti solo i messaggi che quasi certamente sono spam. È molto difficile che un messaggio di posta accettabile abbia un punteggio tanto alto. Il valore predefinito della soglia di rifiuto è 12.

Mostra risultati euristici nei registri di sessioni SMTP
Questa opzione consente di registrare nei registri delle sessioni SMTP 109 i risultati dell'elaborazione euristica eseguita durante le sessioni SMTP.

Invia risultati euristici a client SMTP
Fare clic su questa opzione per mostrare i risultati dell'elaborazione euristica direttamente nelle trascrizioni delle sessioni SMTP. Questa opzione non è disponibile se il valore della soglia di rifiuto del punteggio di spam è impostato a "0", poiché ciò vorrebbe dire che lo spam non viene mai rifiutato per via del punteggio. Per ulteriori informazioni, consultare la precedente sezione "*SMTP rifiuta i msg con punteggi superiori o uguali a XX (0=mai)*".

Salta lo scan dei messaggi processati durante le sessioni SMTP
Per impostazione predefinita, durante la sessione SMTP viene eseguita l'analisi di tutti i messaggi al fine di determinarne il punteggio di spam e scartarli se il punteggio supera la soglia prevista. MDaemon esegue un'ulteriore ricerca in base alle code sui messaggi accettati per definirne la gestione in base ai punteggi e alla configurazione di Spam Filter. Selezionare questa opzione se si desidera escludere la ricerca basata

sulle code e considerare definitivi i risultati della ricerca Spam Filter iniziale. Ciò consente di ridurre considerevolmente l'utilizzo della CPU aumentando le prestazioni del sistema antispam. Se si esclude la ricerca basata sulle code, ai messaggi vengono aggiunte solo le intestazioni SpamAssassin predefinite. Le modifiche alle intestazioni SpamAssassin predefinite o l'aggiunta di specifiche intestazioni personalizzate nel file `local.cf` verranno ignorate.

Respingi il messaggio in caso di errore durante la scansione SMTP
Abilitare questa opzione se si desidera che un messaggio venga rifiutato qualora venga riscontrato un errore durante la sua scansione SMTP.

Tag 'subject'
Questo tag viene inserito all'inizio dell'intestazione Subject (Oggetto) di tutti i messaggi che presentano un valore maggiore o uguale alla soglia del punteggio di spam richiesto. Questa può anche contenere informazioni relative al punteggio di spam ed è possibile utilizzare i filtri dei messaggi IMAP per cercarla e di conseguenza filtrare il messaggio (supponendo che Spam Filter sia configurato in modo da proseguire la consegna dei messaggi spam). Questo è un metodo semplice per instradare automaticamente i messaggi spam in una apposita cartella. Se si desidera inserire dinamicamente il punteggio di spam del messaggio' e il valore della soglia richiesta, utilizzare il tag "`_HITS_`" per il punteggio del messaggio e "`_REQD_`" per la soglia. In alternativa, è possibile utilizzare "`_SCORE(0)_`" al posto di "`_HITS_`"; in questo modo viene aggiunto uno zero iniziale ai punteggi più bassi. Ciò consente di ordinare i messaggi in base all'oggetto in alcuni client e-mail.

Esempio:

Un tag oggetto impostato come `***SPAM*** Score/Req: _HITS_/_REQD_` determina un messaggio spam con un punteggio di 6.2 e la modifica dell'oggetto da "Hey, here's some spam!" in "***SPAM*** Score/Req: 6.2/5.0 – Hey, here's some spam!"

Se "`_SCORE(0)_`" venisse sostituito a "`_HITS_`", il messaggio verrebbe modificato in "***SPAM*** Score/Req: 06.2/5.0 – Hey, here's some spam!"

Se non si desidera alterare l'intestazione, lasciare il campo vuoto in modo da non inserire alcun tag oggetto.

Questa opzione non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. La configurazione del tag "Subject" sarà determinata dalle impostazioni dell'altro server.' Vedere: Spam Daemon 253, per ulteriori informazioni.

Destinazione posta spam

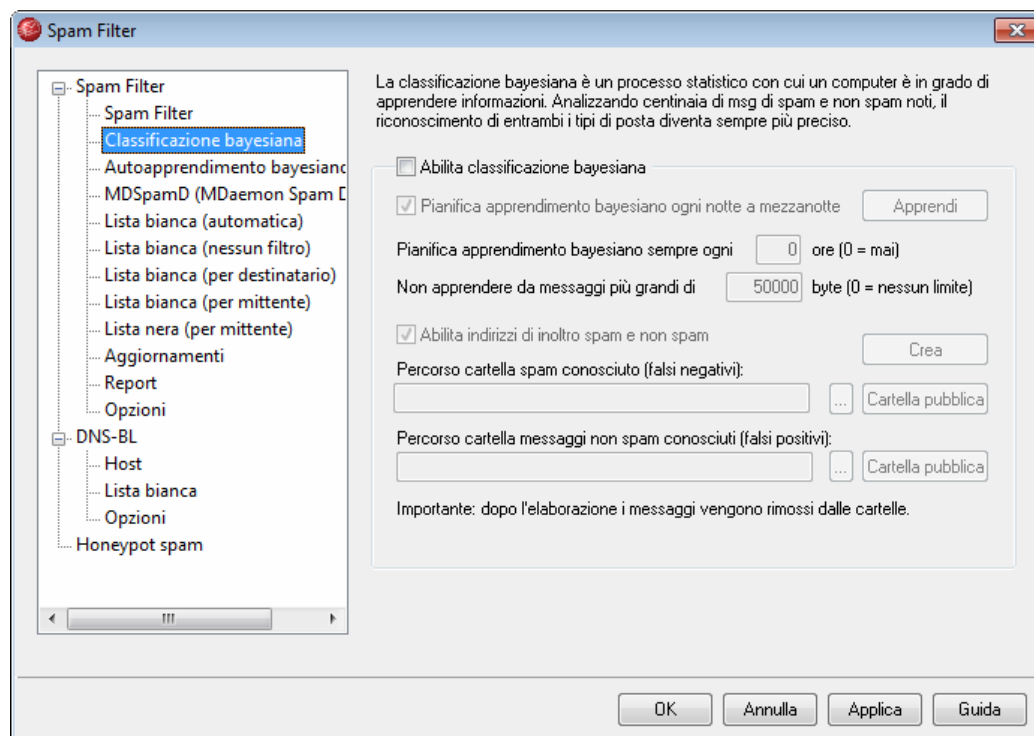
Se il punteggio di spam di un messaggio è maggiore o uguale a quello specificato in precedenza, Spam Filter compie una delle azione elencate di seguito.

Elimina immediatamente
Scegliere questa opzione se si desidera eliminare direttamente tutti i messaggi in arrivo il cui punteggio di spam supera il limite stabilito.

Inserisci messaggio in cartella pubblica spam trap
Scegliere questa opzione se si desidera contrassegnare i messaggi come spam e spostarli nella cartella pubblica spam anziché consentire la loro consegna.

Invia ogni giorno il rapporto spam trap al postmaster
Se si utilizza l'opzione *Inserisci messaggio in cartella pubblica spam trap*, selezionare questa casella di controllo per far sì che il postmaster riceva un messaggio giornaliero con un riepilogo del contenuto della cartella.

contrassegna spam ma lascia proseguire percorso di recapito
Scegliere questa opzione se si desidera proseguire con la consegna di tutti i messaggi spam al destinatario, ma si intende contrassegnarli come tali inserendo le varie intestazioni spam e/o i tag indicati nella schermata Report 264. Questa è l'opzione predefinita e consente di utilizzare opzioni quali lo spostamento della posta in una cartella spam per una revisione successiva evitando così la perdita di messaggi che potrebbero venire contrassegnati erroneamente come indesiderati, ossia dei falsi positivi.

5.3.1.2 Classificazione Bayesiana

Questa opzione non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. Tutti gli apprendimenti bayesiani saranno eseguiti sull'altro server. Per ulteriori informazioni, vedere la schermata Spam Daemon253.

Spam Filter supporta l'apprendimento bayesiano, ovvero un processo statistico che può essere utilizzato per analizzare i messaggi spam e non spam allo scopo di accrescerne nel tempo l'affidabilità nel riconoscimento. È possibile utilizzare una cartella per i messaggi spam e non spam di cui viene effettuata una scansione manualmente oppure automaticamente, a intervalli regolari. Tutti i messaggi contenuti in queste cartelle vengono analizzati e indicizzati in modo da poterli confrontare con i nuovi messaggi e stabilire statisticamente la probabilità che si tratti di messaggi spam. Spam Filter può, quindi, aumentare o diminuire il punteggio di spam del messaggio sulla base dei risultati del confronto bayesiano.

Spam Filter non applica ai messaggi una classificazione bayesiana finché non viene effettuata un'analisi bayesiana sul numero di messaggi spam e non spam specificati nella schermata Autoapprendimento bayesiano251. Ciò serve a fare sì che Spam Filter abbia un insieme di statistiche sufficientemente ampio per iniziare il confronto bayesiano. Una volta ricevuti dal sistema i messaggi da analizzare, questo è pienamente in grado di iniziare ad applicare i dati del confronto bayesiano a ciascun punteggio di spam del messaggio in arrivo. Continuando ad analizzare sempre più messaggi, le classificazioni bayesiane diventano sempre più accurate nel tempo.

Classificazione Bayesiana

Abilita classificazione bayesiana

Fare clic su questa casella di controllo se si desidera che il punteggio di spam di ciascun messaggio venga regolato in base al confronto con le statistiche bayesiane correntemente note.

Pianifica apprendimento bayesiano ogni notte a mezzanotte

Quando questa opzione è attivata, ogni giorno a mezzanotte Spam Filter analizzerà ed eliminerà tutti i messaggi contenuti nelle cartelle Spam e non Spam indicate di seguito. Se si desidera programmare l'apprendimento bayesiano per un altro intervallo di tempo, deselezionare questa opzione e utilizzare l'opzione *Pianifica apprendimento bayesiano sempre ogni XX ore*. Se non si desidera che l'apprendimento bayesiano avvenga automaticamente, deselezionare questa opzione e specificare "0" ore nell'opzione seguente.

Pianifica apprendimento bayesiano sempre ogni XX ore (0 = mai)

Se si desidera che l'apprendimento bayesiano avvenga in un intervallo di tempo diverso da quello di ogni notte a mezzanotte, deselezionare l'opzione descritta in

precedenza e specificare un numero di ore in questa opzione. Quando il numero di ore indicato è trascorso, Spam Filter analizzerà e eliminerà tutti i messaggi contenuti nelle cartelle Spam e non Spam indicate di seguito. Se non si desidera che l'apprendimento bayesiano avvenga sempre automaticamente, deselezionare l'opzione precedente e specificare "0" ore in questa opzione.

Se si desidera conservare i messaggi dopo l'analisi, è possibile creare una copia di `LEARN.BAT` salvandola come `MYLEARN.BAT` nella sottocartella `\MDaemon\App\` ed eliminare quindi le due righe che iniziano con "`if exist`" che si trovano alla fine del file. Se la cartella include il file `MYLEARN.BAT`, MDaemon utilizzerà quest'ultimo anziché il file `LEARN.BAT`. Per ulteriori informazioni, consultare il file `SA-Learn.txt`, situato nella sottocartella `\MDaemon\SpamAssassin\`.

Per informazioni più dettagliate sulla tecnologia euristica dei filtri spam e sull'apprendimento bayesiano, visitare l'indirizzo:

http://www.spamassassin.org/doc/sa-learn.html.

Non apprendere da messaggi più grandi di XX byte (0 = senza lim.)
Questa opzione consente di specificare la dimensione massima del messaggio ai fini dell'analisi bayesiana. I messaggi più grandi di tale dimensione non saranno analizzati. Specificare "0" in questa opzione se non si desidera inserire alcuna limitazione di dimensione.

Apprendi
Fare clic su questo pulsante per avviare manualmente l'analisi bayesiana delle cartelle specificate anziché attendere l'analisi automatica.

Abilita indirizzi di inoltro spam e non spam
Fare clic su questa casella di controllo se si desidera consentire agli utenti l'inoltro di messaggi spam e non spam (ham) a determinati indirizzi per consentire al sistema bayesiano di apprendere da essi. Gli indirizzi predefiniti utilizzati da MDaemon sono "`SpamLearn@<domain.com>`" e "`HamLearn@<domain.com>`". I messaggi inviati a questi indirizzi devono essere ricevuti via SMTP da una sessione autenticata usando SMTP AUTH. Inoltre, MDaemon prevede che i messaggi vengano inoltrati agli indirizzi precedentemente indicati come allegati di tipo "`message/rfc822`". Ogni altro tipo di messaggio inviato a questi indirizzi e-mail non verrà elaborato.

È possibile cambiare gli indirizzi utilizzati da MDaemon aggiungendo la seguente chiave nel file `CFilter.INI`:

```
[SpamFilter]
SpamLearnAddress=IndirizzoApprendimentoSpam@
HamLearnAddress=IndirizzoApprendimentoNonSpam@
```

Nota: l'ultimo carattere di questi valori deve essere "@".

Crea
Fare clic su questo pulsante per creare automaticamente Cartelle IMAP pubbliche 75 spam e non spam e configurarne l'uso da parte di MDaemon. Verranno create le cartelle riportate di seguito.

\Bayesian Learning.IMAP\	Cartella IMAP principale
\Bayesian Learning.IMAP\Spam.IMAP\	Questa cartella è destinata ai falsi negativi, ossia ai messaggi spam con un punteggio non abbastanza elevato per essere considerati tali.
\Bayesian Learning.IMAP\Non-Spam.IMAP\	Questa cartella è destinata ai falsi positivi, ossia ai messaggi non spam con un punteggio errato sufficientemente elevato per essere considerati tali.

Per impostazione predefinita, le autorizzazioni di accesso a queste cartelle sono garantite solo agli utenti di domini locali e sono limitate alle funzioni di ricerca e inserimento. Le autorizzazioni predefinite dell'utente postmaster consentono le funzioni di ricerca, lettura, inserimento ed eliminazione.

Percorso cartella spam conosciuto (falsi negativi)
Questo è il percorso per la cartella usata per l'analisi bayesiana di messaggi spam noti. Copiare in questa cartella solamente i messaggi che si ritengono spam. È opportuno evitare di automatizzare la copia dei messaggi nella cartella, se non utilizzando le opzioni di Autoapprendimento bayesiano 251 o Honeypot spam 273. Se si automatizza tale processo, messaggi non spam potrebbero essere analizzati come spam e ciò diminuirebbe l'affidabilità delle statistiche bayesiane.

Percorso cartella messaggi non spam conosciuti (falsi positivi)
Questo è il percorso per la cartella usata per l'analisi bayesiana di messaggi sicuramente **non** spam. È opportuno copiare in questa cartella solo i messaggi che **non** si ritengono spam. È opportuno evitare di automatizzare la copia dei messaggi nella cartella, se non utilizzando le opzioni di Autoapprendimento bayesiano 251. Se si automatizza tale processo, messaggi spam potrebbero essere analizzati come non spam e ciò diminuirebbe l'affidabilità delle statistiche bayesiane.

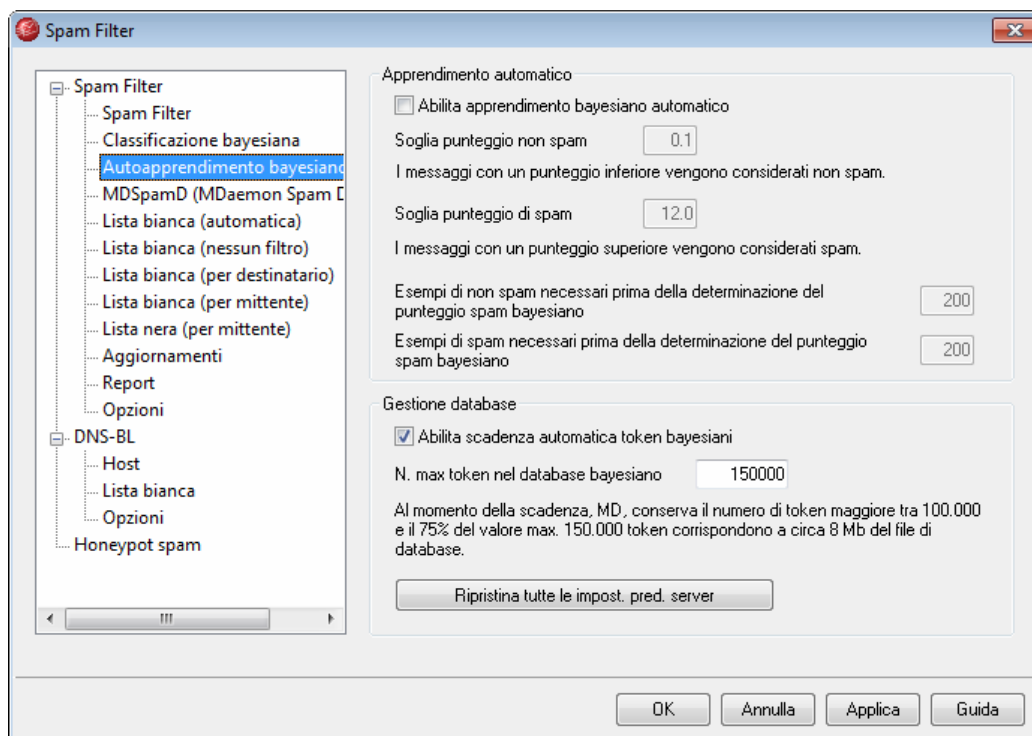
Cartella pubblica
Fare clic su uno dei pulsanti per definire come directory bayesiana una delle cartelle pubbliche esistenti. Si tratta di un metodo semplice per spostare i messaggi erroneamente segnalati come spam o non spam nelle directory bayesiane per l'analisi. Si noti, tuttavia, che autorizzando l'accesso a più persone aumenta la probabilità di inserire i messaggi nelle cartelle errate, alterando le statistiche e diminuendone l'affidabilità.

Se si rinomina una cartella pubblica mediante un client e-mail, Esplora risorse o con altri metodi, è necessario reimpostare manualmente il percorso inserendo il nome corretto della nuova cartella. Se si rinomina una cartella ma non si modifica il percorso nel relativo campo, Spam Filter continua a utilizzare per la cartella bayesiana il vecchio percorso anziché il nuovo.

Per ulteriori informazioni, vedere:

Autoapprendimento bayesiano 251

Honeypot spam 273

5.3.1.3 Autoapprendimento bayesiano

L'autoapprendimento bayesiano non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. Tutti gli apprendimenti bayesiani saranno eseguiti sull'altro server. Per ulteriori informazioni, vedere la schermata Spam Daemon 253.

Apprendimento automatico

Abilita apprendimento bayesiano automatico
Con l'apprendimento bayesiano automatico è possibile indicare le soglie del punteggio spam e non spam che consentono al sistema l'apprendimento automatico dai messaggi, senza la necessità di smistarli manualmente nelle cartelle spam e non spam. Tutti i messaggi con un punteggio inferiore alla soglia non spam sono trattati dall'apprendimento automatico come messaggi accettati mentre i messaggi con un punteggio superiore alla soglia spam sono trattati come messaggi indesiderati. Con l'apprendimento automatico, i vecchi token scaduti e rimossi dal database (vedere *Gestione database*) vengono sostituiti automaticamente. In questo modo non è necessario intervenire manualmente per sostituire i token scaduti. L'autoapprendimento risulta utile e vantaggioso se le soglie sono impostate con attenzione, in modo da evitare che i messaggi vengano collocati nelle cartelle con una classificazione impropria.

Soglia punteggio non spam
Il sistema di Classificazione bayesiana tratta i messaggi con un punteggio di spam inferiore a questo valore come messaggi non spam.

Soglia punteggio di spam
Il sistema di Classificazione bayesiana tratta i messaggi con un punteggio di spam superiore a questo valore come messaggi spam.

Esempi di non spam necessari prima della determinazione del punteggio spam bayesiano
Spam Filter non applica ai messaggi alcuna classificazione bayesiana finché il sistema bayesiano non ha analizzato il numero di messaggi non spam indicati in questo campo e di messaggi spam indicati nell'opzione seguente. Ciò serve a fare sì che Spam Filter abbia un insieme di statistiche sufficientemente ampio per iniziare il confronto bayesiano. Una volta ricevuti dal sistema i messaggi da analizzare, questo è pienamente in grado di iniziare ad applicare i dati del confronto bayesiano a ciascun punteggio di spam del messaggio in arrivo. Continuando ad analizzare sempre più messaggi, le classificazioni bayesiane diventano sempre più accurate nel tempo.

Esempi di spam necessari prima della determinazione del punteggio spam bayesiano
Come per l'opzione precedente relativa ai messaggi non spam, questa definisce il numero di messaggi *spam* da analizzare prima che Spam Filter inizi ad applicare la classificazione bayesiana.

Gestione database

Abilita scadenza automatica token bayesiani
Fare clic su questa opzione se si desidera che i token del database scadano automaticamente una volta raggiunto il numero indicato nel campo successivo. Impostando un limite di token è possibile evitare che il database bayesiano raggiunga dimensioni troppo grandi.

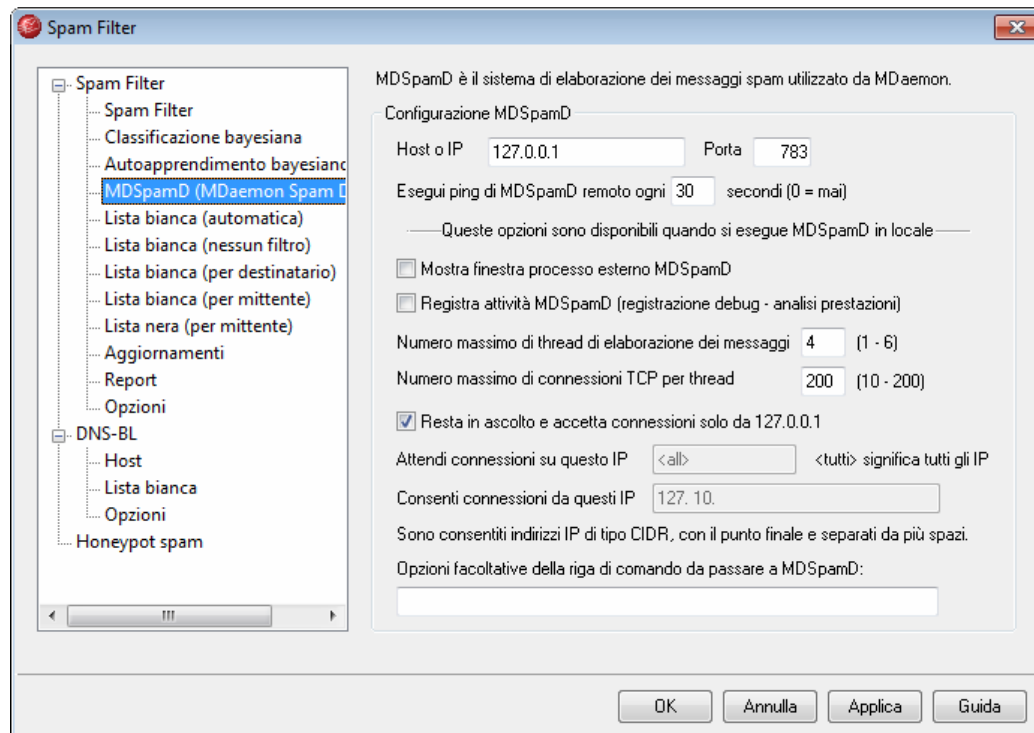
N. max token nel database bayesiano
Questo valore corrisponde al numero massimo di token bayesiani consentiti nel

database. Una volta raggiunto tale numero, il sistema bayesiano elimina i token meno recenti riducendone il numero fino al valore più elevato tra il 75% del valore precedente o 100.000 token. Il numero di token non scende mai al di sotto di questi due valori, indipendentemente dal numero di token scaduti. Nota: 150.000 token del database corrispondono a circa 8 MB.

Ripristina tutte le impostazioni predefinite server
Facendo clic su questo pulsante è possibile ripristinare tutti i valori predefiniti delle opzioni bayesiane avanzate.

Vedere:

Classificazione Bayesiana 247
Honeypot spam 273

5.3.1.4 Spam Daemon (MDSpamD)

Spam Filter di MDaemon viene eseguito come sistema separato, MDSpamD (MDaemon Spam Daemon), a cui vengono inviati i messaggi tramite TCP/IP per la scansione. In questo modo è possibile aumentare le prestazioni di Spam Filter, nonché eseguire MDSpamD nel computer locale, in un altro computer oppure utilizzare un altro servizio MDSpamD (o un qualunque altro prodotto compatibile Spam Daemon) in esecuzione su un'altra postazione. Per impostazione predefinita, MDSpamD viene eseguito localmente e riceve i messaggi sulla porta 783 all'indirizzo 127.0.0.1, ma è possibile configurare una porta e un indirizzo IP differenti se si desidera inviare i messaggi ad un altro Spam Daemon in esecuzione in una postazione diversa o su una porta diversa.

Configurazione MDSpamD

Host o IP
Corrisponde all'host o all'indirizzo IP a cui MDaemon invierà i messaggi da analizzare con MDSpamD. Utilizzare `127.0.0.1` se MDSpamD viene eseguito localmente.

Porta
Corrisponde alla porta a cui il messaggio viene inviato. Il valore predefinito della porta MDSpamD è 783.

Esegui ping di MDSpamD remoto ogni XX secondi (0=mai)
Se si utilizza un servizio antispam (spam daemon) in esecuzione in una postazione remota, questa opzione consente di verificare periodicamente tramite ping se tale servizio è attivo. Inserire "0" se non si desidera effettuare il ping della postazione.

Opzioni disponibili se MDSpamD viene eseguito localmente

Mostra finestra processo esterno MDSpamD
Quando MDSpamD viene eseguito localmente, attivare questa opzione se si desidera eseguirlo in una finestra di processo esterno. Se si abilita questa opzione, l'output generato da MDSpamD viene inviato tramite pipe alla finestra di processo esterno anziché al sistema di registrazione o all'interfaccia utente interna di MDaemon. Questa opzione consente di migliorare le prestazioni perché i dati di MDSpamD non vengono gestiti e registrati da MDaemon. Tuttavia, in questo caso non viene creato alcun file di registro. Di conseguenza, non è possibile utilizzare questa funzione unitamente all'opzione di registrazione descritta successivamente e i dati di MDSpamD non verranno visualizzati nella scheda *Sicurezza»MDSpamD* della finestra principale di MDaemon.

Registra attività MDSpamD (registrazione debug - analisi prestazioni)
Selezionare questa casella di controllo per registrare tutte le attività di MDSpamD. Questa opzione non è disponibile se si utilizza l'opzione *Mostra finestra processo esterno MDSpamD*. Se si utilizzano le credenziali utente specificate nella finestra di dialogo Servizio Windows 205 invece di eseguire MDaemon nell'account SYSTEM, non verrà registrata alcuna attività relativa a MDSpamD.

Se si utilizza questa opzione di registrazione, è possibile che le prestazioni del sistema di posta risultino ridotte, in base al computer in uso e al livello di attività. In genere, è opportuno utilizzare questa opzione solo a scopo di debug.

Numero massimo di thread di elaborazione dei messaggi (1-6)
Corrisponde al numero massimo di thread che saranno utilizzati da MDaemon per l'elaborazione interna. È possibile impostare un valore compreso tra 1 e 6.

Numero massimo di connessioni TCP per thread (10-200)
Corrisponde al numero massimo di connessioni TCP accettate da un thread MDSpamD prima che si dirami in un altro thread. È possibile impostare un valore compreso tra 10 e 200.

Resta in ascolto e accetta connessioni solo da 127.0.0.1
Fare clic su questa opzione se non si desidera consentire al servizio MDSpamD locale di accettare connessioni di qualsiasi origine esterna. Saranno consentite solo connessioni derivanti dalla stessa postazione su cui viene eseguito MDSpamD.

Attendi connessioni su questo IP
Se l'opzione precedente è disattivata, è possibile utilizzare questa opzione per associare o limitare le connessioni ad uno specifico indirizzo IP. Saranno consentite solo le connessioni all'indirizzo IP indicato. Utilizzare "`<all>`" (tutti)" se non si desidera limitare MDSpamD ad un particolare indirizzo IP.

Consenti connessioni da questi IP
Si tratta degli indirizzi IP da cui MDSpamD accetta le connessioni in entrata. Le connessioni da altri indirizzi IP saranno rifiutate. Questa opzione si rivela utile se si desidera consentire connessioni da un altro server per condividere l'elaborazione di Spam Filter.

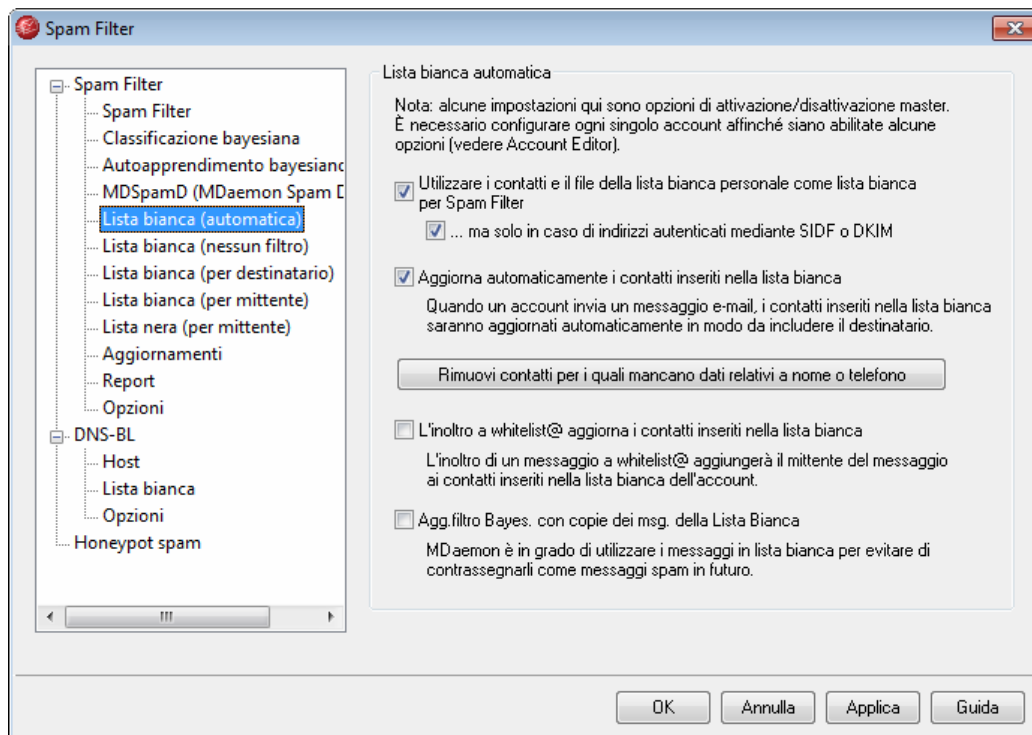
Opzioni facoltative della riga di comando da passare a MDSpamD:

MDSpamD può accettare molte opzioni della riga di comando, descritte nel sito:

http://spamassassin.apache.org/

Se si desidera utilizzare una di queste opzioni, creare una stringa che comprenda le opzioni desiderate e inserirle in questa casella di testo.

È possibile configurare alcune opzioni utilizzando le impostazioni disponibili in questa finestra di dialogo. Di conseguenza, non è necessario impostarle manualmente tramite le opzioni della riga di comando.

5.3.1.5 Lista bianca (automatica)

Lista bianca automatica

Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter
Questa opzione consente agli utenti di utilizzare la cartella Contatti predefinita e la cartella della Lista bianca personale come lista bianca di Spam Filter. Per ogni messaggio in arrivo, MDaemon interroga la lista bianca e i contatti predefiniti di ogni utente alla ricerca del mittente del messaggio. Se il mittente si trova in una delle cartelle, il messaggio viene inserito automaticamente nella lista bianca. Se non si desidera applicare automaticamente questa opzione a tutti gli utenti MDaemon, è possibile disattivarla per singoli utenti, deselezionando l'opzione *Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter* della schermata Opzioni 374 di Account Editor.

Grazie a ComAgent è possibile tenere i contatti aggiornati e sincronizzati con WorldClient, Outlook, Outlook Express, Rubrica di Windows e altri client di posta MAPI che usano la Rubrica di Windows, in modo estremamente semplice.

...ma solo in caso di indirizzi autenticati mediante SIDF o DKIM
Se si abilita questa opzione, MDaemon considererà appartenenti alla lista bianca solo i messaggi il cui mittente sia presente nella lista bianca e che siano autenticati mediante Sender ID Framework 285 (SIDF) o DomainKeys Identified Mail 287 (DKIM). Questa opzione consente di evitare di inserire nella lista bianca messaggi con indirizzi contraffatti.

Aggiorna automaticamente i contatti inseriti nella lista bianca
Se si abilita questa opzione, MDaemon aggiunge automaticamente alla cartella Lista bianca personale tutti gli indirizzi di posta elettronica remoti ai quali vengano inviati messaggi. Se utilizzata unitamente all'opzione "*Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter*", è possibile ridurre sensibilmente il numero di messaggi falsi positivi di Spam Filter.

Se non si desidera applicare automaticamente questa opzione a tutti gli utenti MDaemon, è possibile disattivarla per singoli utenti, deselezionando la casella di controllo "*Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter*" della schermata Opzioni374 di Account Editor.

Questa opzione è disattivata per gli account che usano risposte automatiche.

Rimuovi contatti per i quali mancano dati relativi a nome o telefono
Questo pulsante consente di rimuovere dalla cartella Contatti predefinita degli utenti tutti i contatti che contengono solo l'indirizzo di posta elettronica. I contatti privi del nome o dei dati telefonici vengono rimossi. Questa opzione agevola coloro che hanno utilizzato l'opzione della lista bianca automatica di MDaemon prima che la versione 11 eliminasse i contatti aggiunti solo in virtù della lista bianca. Nelle versioni di MDaemon precedenti, gli indirizzi venivano aggiunti ai contatti principali, anziché a una cartella lista bianca dedicata. Ciò può comportare un esubero di voci nella cartella dei contatti degli utenti che sarebbe preferibile evitare.

È consigliabile utilizzare questa opzione con grande cautela, perché i contatti contenenti solo l'indirizzo di posta elettronica potrebbero essere legittimi.

L'inoltro a whitelist@ aggiorna i contatti inseriti nella lista bianca
Se si abilita questa opzione, gli account impostati su "*Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter*" della schermata Opzioni di Account Editorpossono inoltrare messaggi a `whitelist@<dominio.com>` per aggiungere automaticamente il mittente del messaggio originale alla lista bianca dell'account. L'indirizzo inserito nella lista bianca viene ricavato dall'intestazione `From` del messaggio inoltrato.

I messaggi inoltrati a `whitelist@<dominio.com>` devono essere allegati di tipo `message/rfc822` e devono pervenire a MDaemon tramite SMTP da una sessione autenticata. I messaggi inoltrati che non soddisfano tali requisiti non vengono elaborati.

È possibile cambiare gli indirizzi utilizzati da MDaemon modificando la seguente chiave nel file `CFILTER.INI`:

```
[SpamFilter]
WhiteListAddress=MyWhiteListAddress@
```

Nota: l'ultimo carattere deve essere "@".

Aggiorna filtro Bayesiano con copie dei msg della Lista Bianca
Fare clic su questa casella per copiare automaticamente i messaggi autorizzati nella cartella di apprendimento bayesiano non spam, specificata nella schermata Bayesiano 247. Ciò consente di offrire automaticamente al motore bayesiano esempi di posta non spam. Fornendo regolarmente al motore bayesiano esempi di non spam da cui apprendere, se ne accresce nel tempo l'affidabilità e ciò consente di ridurre il numero di messaggi erroneamente classificati come spam.

Perché questa funzione sia disponibile, è necessario che il messaggio in entrata sia indirizzato a un utente locale e che il mittente sia presente nel file della rubrica. Se il messaggio è in uscita, è necessario invece che il destinatario sia presente nella rubrica. Se non si desidera autorizzare alcun messaggio in uscita, utilizzare Blocco note per modificare la seguente impostazione nel file `MDaemon.ini`:

```
[SpamFilter]
UpdateHamFolderOutbound=No (valore predefinito = Yes)
```

Se il messaggio è autorizzato, viene copiato nella cartella di apprendimento bayesiano non spam anche se non è stato attivato l'apprendimento pianificato nella schermata Bayesiano. In questo modo, se l'apprendimento pianificato o quello manuale vengono successivamente attivati, sarà pronto un insieme di messaggi non spam per l'analisi. Tuttavia, non tutti i messaggi autorizzati vengono copiati nella cartella di apprendimento. Se è stata attivata questa funzione, MDaemon copia i messaggi autenticati fino al raggiungimento di un numero stabilito e successivamente copia i messaggi a intervalli prestabiliti. Per impostazione predefinita, inizialmente vengono copiati i primi 200 messaggi autenticati e poi, successivamente, dieci alla volta. Il numero iniziale di copie è quello specificato nell'opzione "*Esempi di non spam necessari prima della determinazione del punteggio spam bayesiano*" della schermata Autoapprendimento bayesiano 251. Modificando l'impostazione si modifica anche questo valore. Per modificare l'intervallo con cui vengono copiati i messaggi successivi, modificare la seguente impostazione del file `MDaemon.ini`:

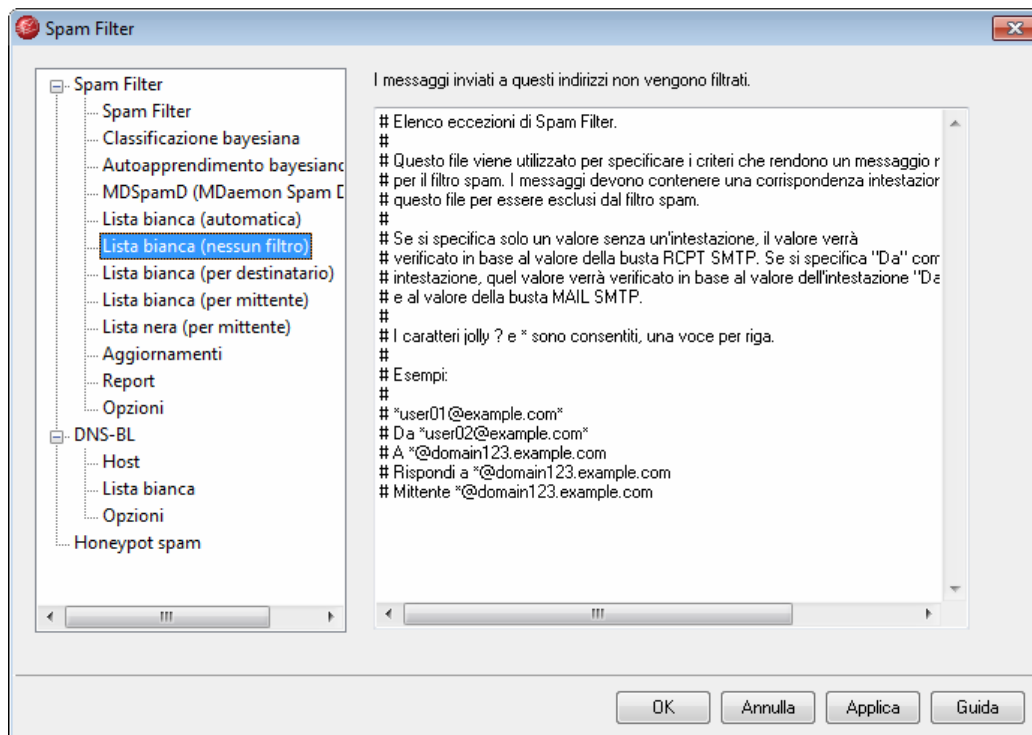
```
[SpamFilter]
HamSkipCount=10 (valore predefinito = 10)
```

Infine, al termine della copia dei messaggi specificati, l'intero processo riprende nuovamente; inizialmente ne vengono copiati 200 e poi dieci alla volta o un altro valore se questa impostazione è stata modificata. Per impostazione predefinita, il processo viene riavviato dopo che sono stati copiati 500 messaggi autenticati. È possibile modificare questo valore cambiando la seguente impostazione nel file `MDaemon.ini`:

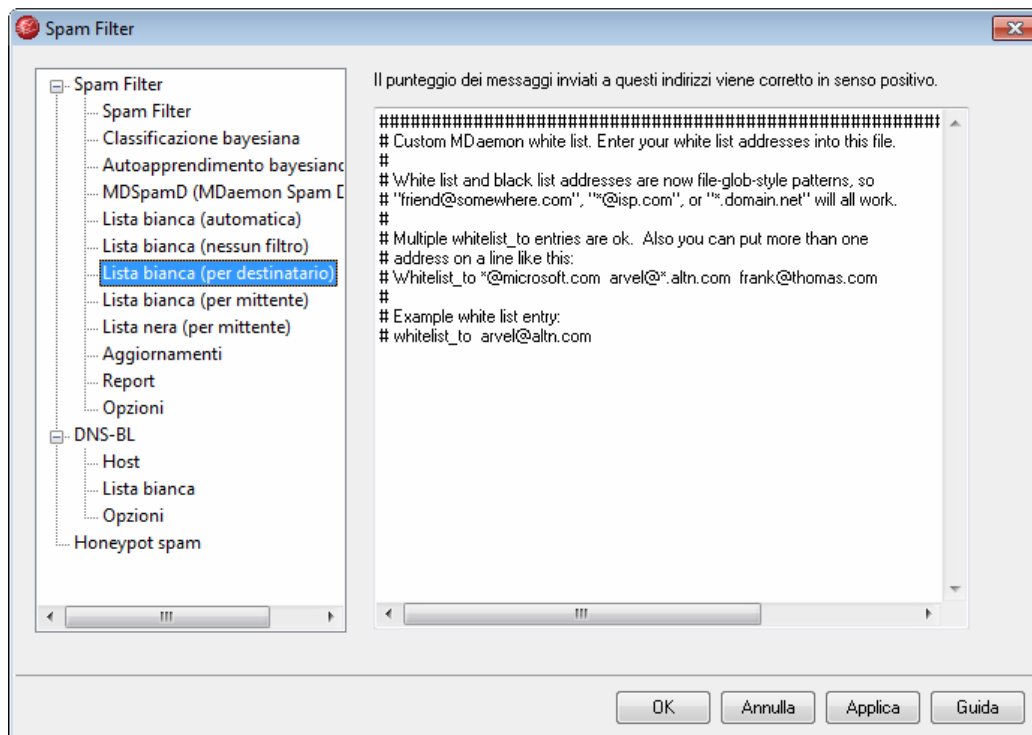
```
[SpamFilter]
HamMaxCount=500 (valore predefinito = 500)
```

Questa opzione non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam

Filter. Tutte le funzioni di apprendimento bayesiano vengono determinate dalle impostazioni dell'altro server ed eseguite da esso. Per ulteriori informazioni, vedere Spam Daemon 253.

5.3.1.6 Lista bianca (nessun filtro)

I messaggi inviati a questi indirizzi non vengono filtrati.
Utilizzare questa schermata per specificare gli indirizzi dei destinatari ai quali non si desidera applicare filtri spam. I messaggi destinati a questi indirizzi non vengono elaborati mediante filtri spam.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. In questo caso, l'elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 253.

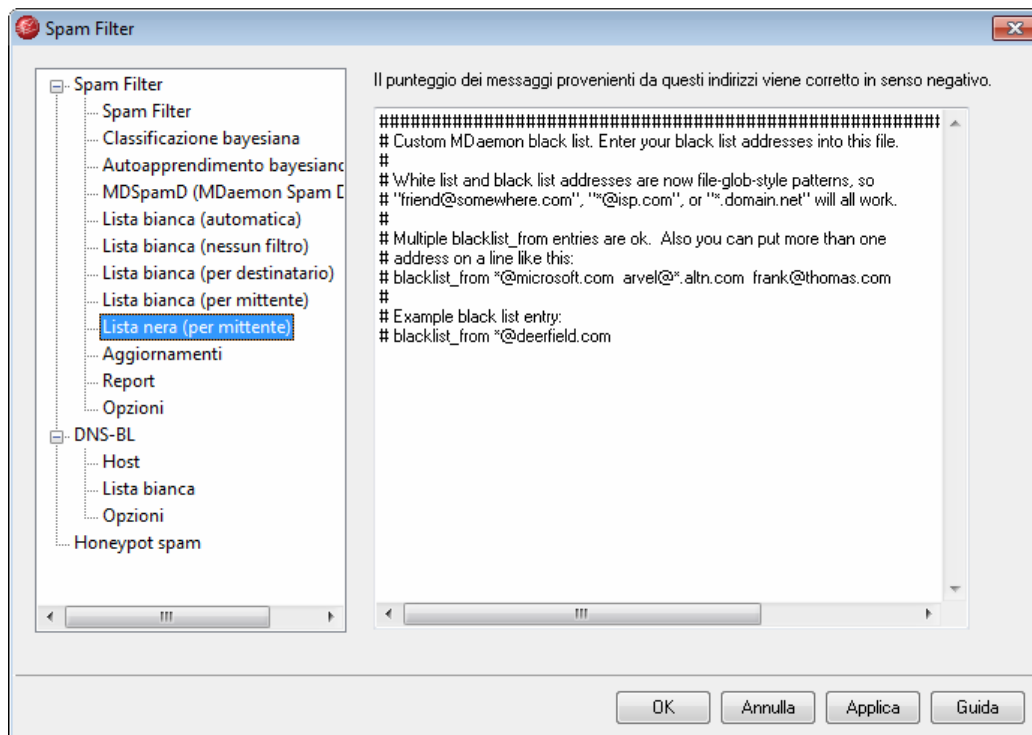
5.3.1.7 Lista bianca (per destinatario)

Il punteggio dei messaggi inviati a questi indirizzi viene corretto in senso positivo.
L'inserimento di un indirizzo in una lista bianca non garantisce automaticamente che un messaggio destinato a quell'indirizzo non venga considerato spam. Al contrario, dal punteggio di spam dei messaggi inviati a indirizzi contenuti nella lista bianca viene sottratto il valore specificato nella schermata Spam Filter 244. Ad esempio, se la soglia del punteggio spam è impostata su 5.0, il valore della lista bianca è impostato su 50 e a uno specifico messaggio spam in arrivo viene assegnato un punteggio spam maggiore o uguale a 55.0 prima di sottrarvi il valore della lista bianca, il punteggio finale corrisponderà almeno a 5.0 e ciò lo contrassegnerà come messaggio spam. Questa eventualità è tuttavia abbastanza rara, in quanto i messaggi spam difficilmente raggiungono un punteggio così elevato a meno che non contengano elementi che fanno salire eccezionalmente il punteggio, ad esempio un indirizzo inserito in una lista nera.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. In questo caso, l'elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 253.

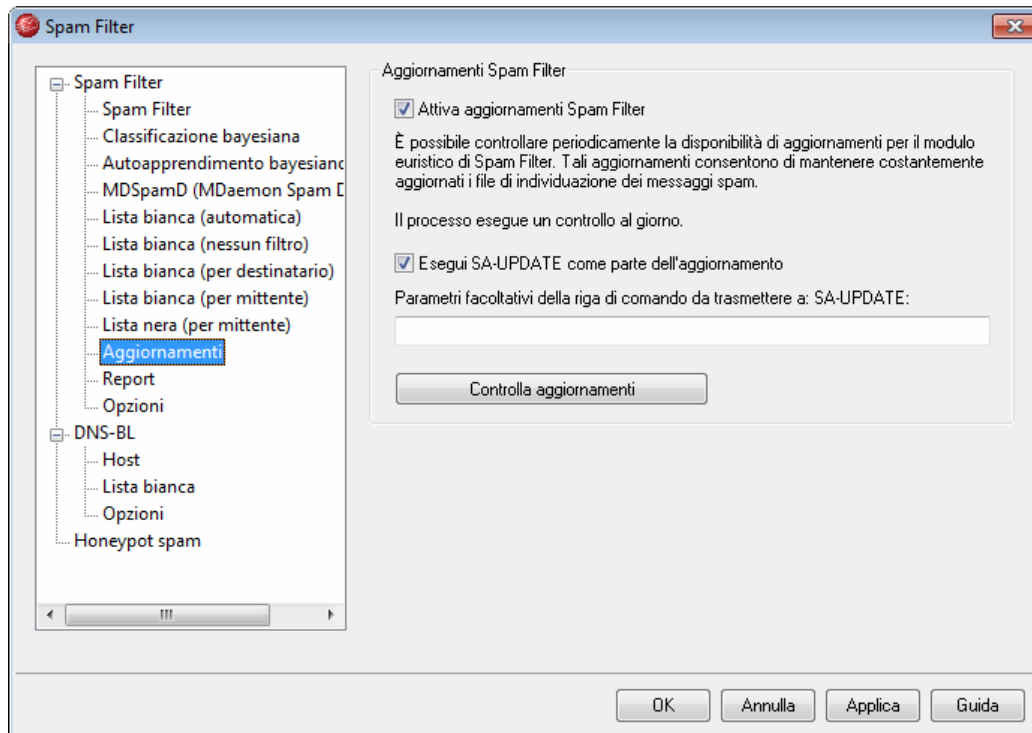
5.3.1.8 Lista bianca (per mittente)

Il punteggio dei messaggi provenienti da questi indirizzi viene corretto in senso positivo.
L'inserimento di un indirizzo in una lista bianca non garantisce automaticamente che un messaggio proveniente da quell'indirizzo non venga considerato spam. Al contrario, dal punteggio di spam dei messaggi provenienti da indirizzi contenuti nella lista bianca viene sottratto il valore specificato nella schermata Spam Filter 244. Ad esempio, se la soglia del punteggio spam è impostata su 5.0, il valore della lista bianca è impostato su 50 e a uno specifico messaggio spam in arrivo viene assegnato un punteggio spam maggiore o uguale a 55.0 prima di sottrarvi il valore della lista bianca, il punteggio finale corrisponderà almeno a 5.0 e ciò lo contrassegnerà come messaggio spam. Questa eventualità è tuttavia abbastanza rara, in quanto i messaggi spam difficilmente raggiungono un punteggio così elevato a meno che non contengano elementi che fanno salire eccezionalmente il punteggio, ad esempio un indirizzo inserito in una lista nera.

Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. Questo elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 253.

5.3.1.9 Lista nera (per mittente)

Il punteggio dei messaggi provenienti da questi indirizzi viene corretto in senso negativo.
L'inserimento di un indirizzo in una lista nera non garantisce automaticamente che un messaggio proveniente da quell'indirizzo venga considerato spam. Al contrario, al punteggio di spam dei messaggi provenienti da indirizzi contenuti nella lista nera viene aggiunto il valore specificato nella schermata Spam Filter 244. Ad esempio, se la soglia del punteggio di spam è impostata su 5.0, il valore della lista nera della scheda Spam Filter è impostato su 50 e a uno specifico messaggio viene assegnato un punteggio spam inferiore o uguale a -50.0 prima di aggiungervi il valore della lista nera, il punteggio finale corrisponderà almeno a 5.0 e ciò lo contrassegnerà come messaggio non spam legittimo. Questa eventualità, tuttavia, è abbastanza rara poiché ai punteggi di spam dei messaggi difficilmente viene sottratto un valore simile a meno che non contengano altri elementi speciali, ad esempio un indirizzo contenuto in una lista bianca.

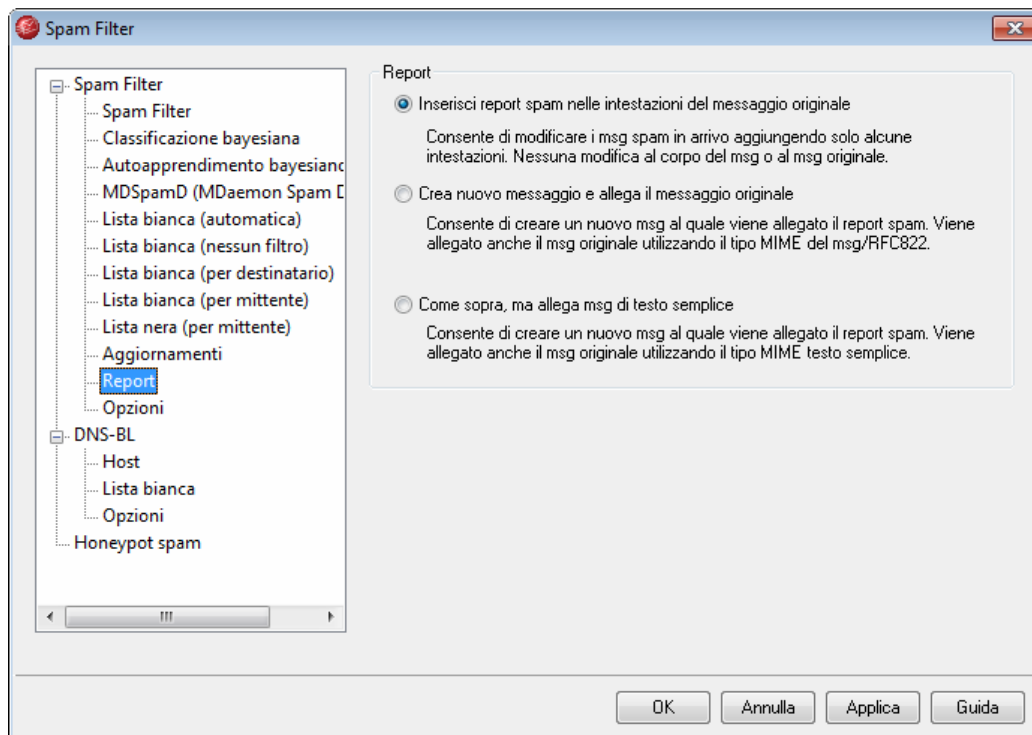
Questa schermata non è disponibile se MDaemon è stato configurato per utilizzare il servizio MDaemon Spam Daemon (MDSpamD) di un altro server ai fini delle elaborazioni di Spam Filter. In questo caso, l'elenco di Spam Filter viene gestito sull'altro server. Per ulteriori informazioni, vedere Spam Daemon 253.

5.3.1.10 Aggiornamenti

Aggiornamenti Spam Filter

Attiva aggiornamenti Spam Filter
Selezionare questa casella di controllo se si desidera che Spam Filter venga aggiornato automaticamente. MDaemon controllerà una volta al giorno la disponibilità di aggiornamenti del modulo euristico di Spam Filter e, se tali aggiornamenti sono disponibili, li scaricherà e li installerà automaticamente.

Esegui SA-UPDATE come parte dell'aggiornamento
Selezionare questa casella di controllo per ricevere gli aggiornamenti da `updates.spamassassin.org` oltre a quelli di Alt-N Technologies. Questa funzione garantisce l'aggiornamento costante delle regole di SpamAssassin.

Controlla aggiornamenti
Fare clic su questo pulsante per verificare in modo immediato se è disponibile un aggiornamento delle regole Spam Filter.

5.3.1.11 Report

Le opzioni di reportistica di Spam Filter non sono disponibili quando MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. La reportistica di Spam Filter verrà controllata dalle impostazioni dell'altro server. Per ulteriori informazioni, vedere la schermata Spam Daemon 253.

Report

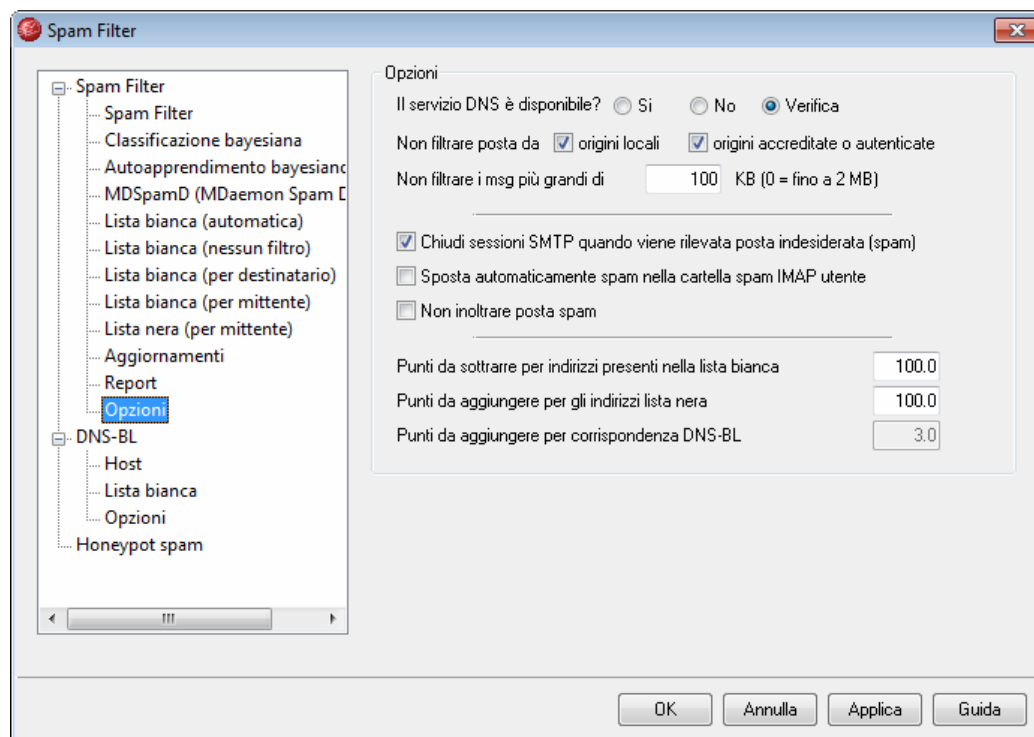
Inserisci report spam nelle intestazioni del messaggio originale
Questa è l'impostazione predefinita. Scegliere questa opzione se si desidera che Spam Filter inserisca un report di spam in ciascuna intestazione dei messaggi spam. Quanto segue è un esempio di report di spam di base:

```
X-Spam-Report: ---- Start Spam Filter results
 5.30 points, 5 required;
 * -5.7 -- Message-Id indicates the message was sent from MS Exchange
 * 2.0 -- Subject contains lots of white space
 * -3.3 -- Has a In-Reply-To header
 * 3.0 -- Message has been marked by MDaemon's DNS-BL
* 2,9 -- BODY: Impotence cure
* 2,2 -- BODY: Talks about exercise with an exclamation!
* 0,5 -- BODY: Message is 80% to 90% HTML
* 0,1 -- BODY: HTML included in message
* 1,6 -- BODY: HTML message is a saved web page
* 2.0 -- Date: is 96 hours or more before Received: date
```

```
---- End of Spam Filter results
```

Crea nuovo messaggio e allega il messaggio originale
Scegliere questa opzione se si desidera che la posta spam generi un nuovo messaggio e-mail contenente un report di spam. Il messaggio spam originale viene incluso come file allegato.

Come sopra, ma allega msg di testo semplice
Come l'opzione precedente, questa genera un report di spam sotto forma di nuovo messaggio e include il messaggio spam originale come file allegato. La differenza consiste nell'allegare il messaggio originale con il tipo MIME text/plain. Dal momento che la posta spam contiene a volte codice HTML, differente per ciascun messaggio e può potenzialmente rivelare allo "spammer" l'indirizzo IP e l'indirizzo e-mail di chi apre il messaggio, questo metodo consente di evitare che ciò avvenga convertendo il codice HTML in semplice testo.

5.3.1.12 Opzioni

Il servizio DNS è disponibile?
Queste opzioni consentono di scegliere se utilizzare o meno il servizio DNS per Spam Filter durante l'elaborazione dei messaggi. È possibile scegliere una delle opzioni seguenti:

Sì - Il servizio DNS è disponibile. Di conseguenza, verranno utilizzate le funzioni SURBL/RBL e le altre regole che richiedono una connessione DNS.

No - Il servizio DNS non è disponibile. Non verranno utilizzate le regole di Spam

Filter che richiedono una connessione DNS.

Verifica - Consente di verificare la disponibilità del servizio DNS che, se presente, verrà utilizzato. Questa è l'impostazione predefinita.

Non filtrare posta da

origini locali
Selezionare questa casella di controllo se si desidera escludere dal filtro spam i messaggi inviati da utenti e domini locali.

origini accreditate o autenticate
Attivare questa opzione se si desidera escludere dal filtro spam i messaggi inviati da domini accreditati o autenticati.

Non filtrare i msg più grandi di XX KB (0=fino a 2 MB)
Solitamente i messaggi spam sono di dimensioni abbastanza ridotte poiché l'obiettivo comune dei cosiddetti "spammer" è quello di consegnare il maggior numero di messaggi nel minor tempo possibile. Se si desidera escludere dal filtro spam i messaggi che superano una determinata dimensione, specificarla in questo campo (in KB). Inserire il valore "0" se non si desidera utilizzare la dimensione come fattore determinante nell'esclusione dal filtro spam. In questo caso i messaggi vengono elaborati dal filtro spam senza tener conto della dimensione.

Chiudi sessioni SMTP quando viene rilevata posta indesiderata (spam)
Questa opzione è abilitata per impostazione predefinita e determina la chiusura di una sessione SMTP qualora l'analisi in linea rilevi un messaggio spam.

Sposta automaticamente spam nella cartella spam IMAP utente
Selezionare questa opzione se si desidera che MDaemon sposti automaticamente i messaggi riconosciuti come posta indesiderata da Spam Filter nella cartella IMAP "`Spam`" relativa all'utente, se questa esiste. In questo modo viene creata automaticamente una cartella per ogni nuovo account utente.

Facendo clic su questa opzione è possibile scegliere se generare o meno questa cartella per tutti gli account utente già esistenti. Se si sceglie "Sì" viene creata una cartella per tutti gli utenti, mentre se si sceglie "No" viene creata una cartella solo quando si aggiunge un nuovo utente. Tutte le cartelle degli utenti già esistenti non subiscono alcuna variazione o modifica.

Non inoltrare posta spam
Selezionare questa casella di controllo se si desidera consentire l'inoltro di messaggi spam.

Le opzioni rimanenti di questa schermata non sono disponibili se MDaemon è stato configurato per utilizzare il servizio MDSpamD (MDaemon Spam Daemon) di un altro server ai fini delle elaborazioni di Spam Filter. Per ulteriori informazioni, vedere la schermata Spam Daemon 253.

Punti da sottrarre per indirizzi presenti nella lista bianca
L'inserimento di un indirizzo nella schermata Lista bianca (per destinatario) 260 o Lista bianca (per mittente) 261 di Spam Filter non garantisce automaticamente che un messaggio proveniente o destinato a quell'indirizzo non venga considerato spam. Al contrario, al punteggio spam degli indirizzi inseriti nelle liste bianche sarà sottratto il punteggio indicato in questo campo. Ad esempio, se la soglia del punteggio di spam è impostata a 5.0 e questo valore è impostato a 100 allora la quantità di messaggi spam in arrivo è alquanto elevata e raggiunge un punteggio di spam maggiore o uguale a 105.0 prima di sottrarvi il valore della lista bianca, dunque il punteggio di spam finale del messaggio corrisponde almeno a 5.0 che porta a riconoscere il messaggio come spam. Questa eventualità è tuttavia abbastanza rara, in quanto i messaggi spam difficilmente raggiungono un punteggio così elevato, a meno che non contengano elementi che fanno salire eccezionalmente il punteggio, ad esempio un indirizzo inserito in una lista nera. Naturalmente, se si imposta un valore da sottrarre inferiore, allora ciò avviene più frequentemente.

Se si desidera che i messaggi indirizzati ad alcuni destinatari vengano completamente esclusi da Spam Filter, includere gli indirizzi dei destinatari nell'elenco che si trova nella schermata Lista bianca (nessun filtro) 259. È inoltre possibile escludere in base al mittente i messaggi dal punteggio di Spam Filter utilizzando le opzioni della schermata Lista bianca (automatica) 256.

Punti da aggiungere per gli indirizzi lista nera
Questo valore viene aggiunto al punteggio spam dei messaggi inviati dagli indirizzi presenti nella schermata Lista nera (per mittente) 262. Come per le opzioni descritte in precedenza relative alle liste bianche, l'inserimento di un indirizzo nella lista nera di Spam Filter non garantisce automaticamente che un messaggio proveniente da quell'indirizzo venga considerato spam. Al contrario, il valore indicato in questo campo viene aggiunto al punteggio di spam del messaggio e utilizzato quindi per determinare se un messaggio debba essere considerato spam.

Punti da aggiungere per corrispondenza DNS-BL
Se si utilizzano le Liste nere DNS 267, questa opzione consente di specificare un valore da aggiungere al punteggio di spam del messaggio nel caso di corrispondenza con le liste nere DNS. A volte il controllo euristico di un messaggio da parte di Spam Filter può dare un risultato non sufficientemente alto da essere considerato spam, mentre una ricerca nelle liste nere DNS (DNS-BL) è in grado di determinare che si tratta di spam. L'aggiunta di questo valore al punteggio di spam dei messaggi consente di ridurre il numero di messaggi spam che riescono a sfuggire al rilevamento da parte di Spam Filter.

5.3.2 Liste nere DNS (DNS-BL)

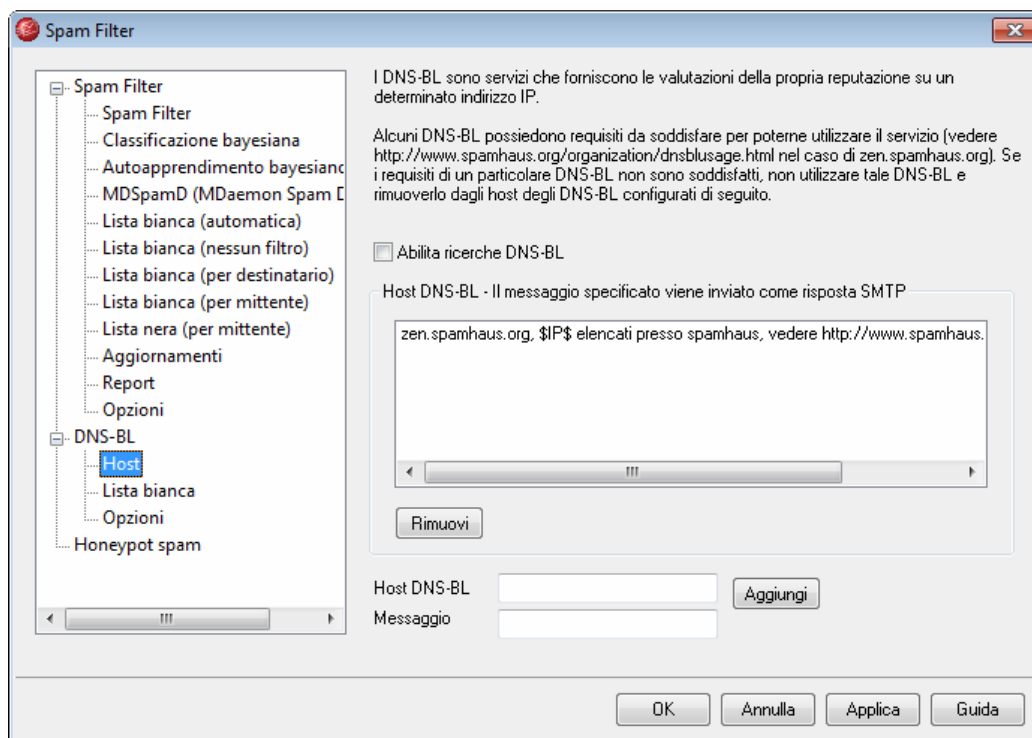
Le Liste nere DNS (DNS-BL) possono impedire a parte dei messaggi e-mail indesiderati di raggiungere le caselle postali degli utenti. Questa funzione di sicurezza consente di specificare numerosi servizi relativi a liste nere DNS (che gestiscono appositi elenchi di

server noti per inoltrare posta indesiderata) che vengono consultati ogni volta che un messaggio viene inviato al server. Se l'indirizzo IP che richiede la connessione è presente sulla lista nera di uno qualsiasi di questi servizi, il messaggio o i messaggi vengono respinti o contrassegnati in base alle impostazioni della schermata Opzioni 270.

Le liste nere DNS contengono, inoltre, un database delle eccezioni o Lista bianca, in cui sono presenti gli indirizzi IP esclusi dal controllo. Prima di attivare la funzione DNS-BL, assicurarsi che l'intervallo degli indirizzi IP locali sia inserito nella lista bianca per escluderli dalle ricerche; l'indirizzo "127.0.0.1" è già escluso e non è necessario aggiungerlo alle eccezioni.

Per ulteriori informazioni, vedere:

Host DNS-BL 268
Opzioni DNS-BL 270
Lista bianca DNS-BL 269

5.3.2.1 Host

Host DNS-BL

Abilita ricerche DNS-BL
Attivare questa opzione se si desidera controllare la posta in arrivo a fronte delle liste nere DNS. Durante la ricerca DNS-BL dell'indirizzo IP mittente, MDaemon interroga ciascuno degli host presenti nell'elenco. Se un host risponde all'interrogazione con esito positivo, MDaemon può apporre un flag al messaggio o rifiutare di accettarlo, in base alle opzioni selezionate nella schermata Opzioni 270 di

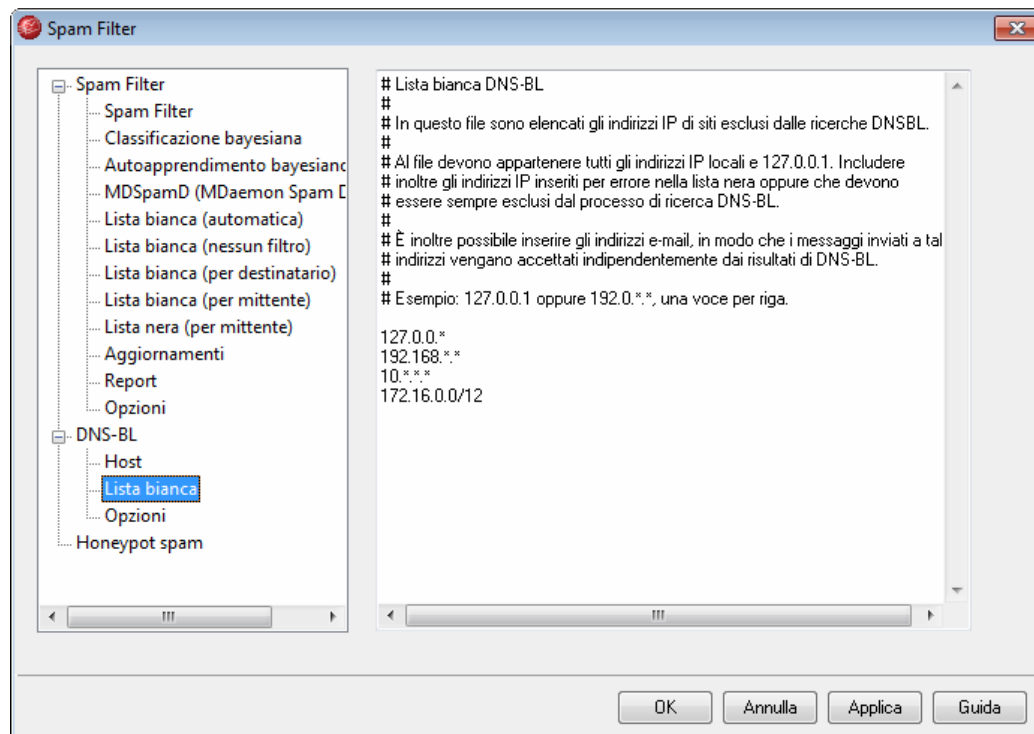
DNS-BL.

Rimuovi
Selezionare una voce dall'elenco dei servizi DNS-BL, quindi premere questo pulsante per rimuoverla dall'elenco.

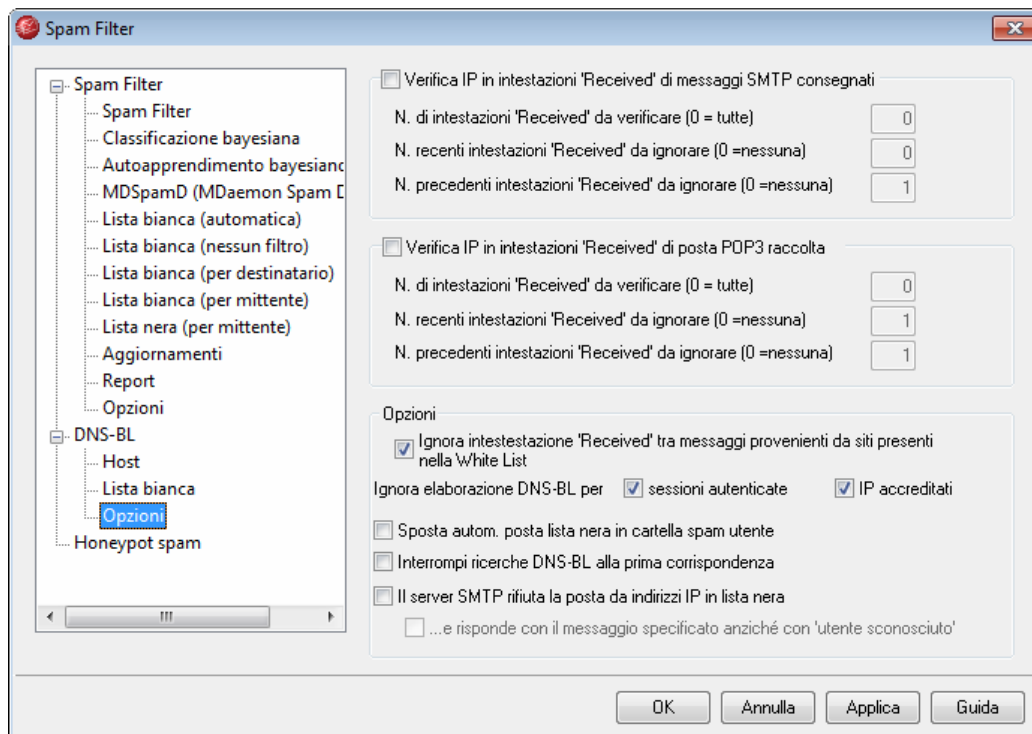
Host DNS-BL
Immettere in questo campo il nome del nuovo host da interrogare per la ricerca di indirizzi IP contenuti nelle liste nere.

Messaggio
Si tratta del messaggio che viene inviato durante la sessione SMTP, quando un indirizzo IP risulta nella lista nera associata all'host DNS-BL corrispondente. Tale messaggio corrisponde all'opzione *...e risponde con il messaggio specificato anziché con 'utente sconosciuto'* della schermata Opzioni270 di DNS-BL.

Aggiungi
Una volta immesso l'host e il messaggio da restituire, fare clic su questo pulsante per aggiungere la voce all'elenco degli host DNS-BL.

5.3.2.2 Lista bianca

Questa schermata consente di specificare gli indirizzi IP esenti dalle ricerche nelle liste nere DNS (DNS-BL). È opportuno includere sempre l'indirizzo IP locale per impedire che il servizio DNS-BL effettui ricerche sui messaggi originati da utenti e domini locali, ossia `127.0.0.*`, `192.168.*.*` e così via. Inserire un indirizzo per ogni riga. I caratteri jolly

sono accettati.

5.3.2.3 Opzioni

Verifica IP in intestazioni 'Received' di messaggi SMTP consegnati
Selezionare questa opzione se si desidera che la funzione liste nere DNS (DNS-BL) verifichi l'indirizzo IP inserito nelle intestazioni "Received" dei messaggi ricevuti via SMTP.

N. di intestazioni 'Received' da verificare (0 = tutte)
Specificare il numero di intestazioni "Received" da sottoporre alla verifica DNS-BL, a partire dal messaggio più recente. Con il valore "0", vengono verificate tutte le intestazioni "Received".

N. recenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che la funzione DNS-BL ignori le intestazioni Received più recenti durante la verifica dei messaggi SMTP, utilizzare questa opzione.

N. precedenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che le intestazioni "Received" meno recenti vengano ignorate durante la verifica dei messaggi SMTP, utilizzare questa opzione.

Verifica IP in intestazioni 'Received' di posta POP3 raccolta
Se questa opzione è abilitata, la funzione DNS-BL verifica l'indirizzo IP inserito nell'intestazione "Received" dei messaggi raccolti tramite DomainPOP e MultiPOP.

N. di intestazioni 'Received' da verificare (0 = tutte)
Specificare il numero di intestazioni 'Received' da sottoporre alla verifica DNS-BL, a partire dal messaggio più recente. Con il valore "0", vengono verificate tutte le intestazioni 'Received'.

N. recenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che la funzione DNS-BL ignori le intestazioni Received più recenti durante la verifica dei messaggi DomainPOP e MultiPOP, utilizzare questa opzione. Poiché risulta spesso necessario ignorare l'intestazione Received più recente della posta POP3 raccolta, ad esempio DomainPOP, per impostazione predefinita a questa opzione è assegnato il valore "1".

N. precedenti intestazioni 'Received' da ignorare (0 =nessuna)
Se si desidera che le intestazioni "Received" meno recenti vengano ignorate durante la verifica dei messaggi DomainPOP e MultiPOP, utilizzare questa opzione.

Opzioni

Ignora intestazione 'Received' tra messaggi provenienti da siti presenti nella White list
Se questa opzione è abilitata, la funzione DNS-BL non verifica le intestazioni "Received" dei messaggi provenienti dagli indirizzi IP specificati in Lista bianca DNS-BL 269.

Ignora elaborazione DNS-BL per:

sessioni autenticate
Fare clic su questa casella di controllo per escludere dalla ricerca delle DNS-BL le sessioni autenticate mediante il comando AUTH.

IP accreditati
Fare clic su questa casella di controllo per escludere dalla ricerca delle DNS-BL gli indirizzi elencati nella schermata Host accreditati 282.

Interrompi ricerche DNS-BL alla prima corrispondenza
Nelle intestazioni di ciascun messaggio elaborato dai servizi DNS-BL sono spesso presenti più host e anche i servizi DNS-BL interrogati sono numerosi. Per impostazione predefinita, queste ricerche interrogano tutti i servizi disponibili al fine di individuare tutti gli host presenti nel messaggio, senza tener conto del numero di corrispondenze trovate. Fare clic su questa opzione se si desidera che le ricerche DNS-BL relative a un messaggio vengano interrotte appena viene trovata una corrispondenza.

Il server SMTP rifiuta la posta da indirizzi IP in lista nera
Per impostazione predefinita, questa opzione è disattivata in modo che i messaggi provenienti dagli indirizzi IP della lista nera non vengano rifiutati durante la sessione SMTP, ma vengano contrassegnati con l'intestazione X-MDDNSBL-Result. Sarà poi sufficiente utilizzare la funzione Filtro contenuti per trovare i messaggi con tale intestazione e destinarli di conseguenza. Per il filtro automatico dei messaggi nella cartella Spam di ciascun utente, è inoltre possibile utilizzare l'opzione "*Sposta autom. posta lista nera in cartella spam utente*" descritta successivamente. Se si desidera che MDaemon rifiuti i messaggi provenienti dagli indirizzi della lista nera,

anziché contrassegnarli, abilitare questa opzione.

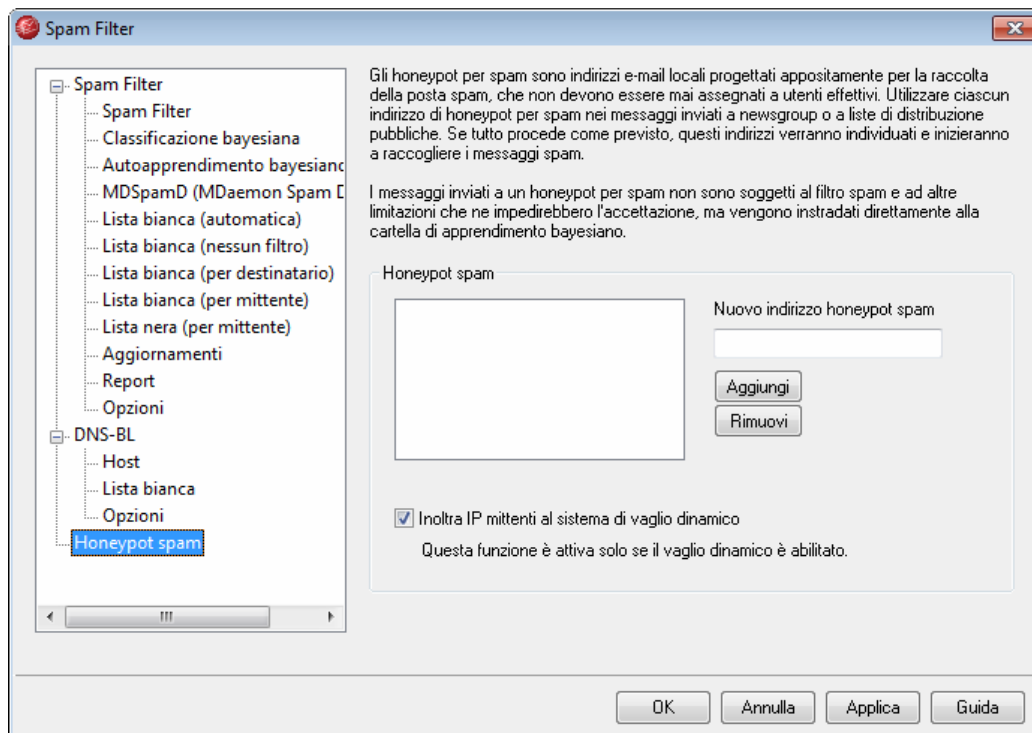
Poiché alcuni indirizzi IP potrebbero essere stati inclusi nella lista nera per errore, è necessario essere cauti nella scelta di rifiutare i messaggi anziché contrassegnarli. Si noti inoltre che, oltre a contrassegnare un messaggio, è possibile modificarne il punteggio spam sulla base dei risultati DNS-BL mediante l'opzione *Punti da aggiungere per corrispondenza DNS-BL* situata in Spam Filter 244.

...e risponde con il messaggio specificato anziché con 'utente sconosciuto'
Fare clic su questa opzione se si desidera che un determinato messaggio assegnato all'host DNS-BL 268 venga trasmesso durante la sessione SMTP ogni volta che un indirizzo IP viene individuato in una lista nera. In caso contrario, viene trasmesso il messaggio "user unknown". Questa opzione è disponibile solo se si è attivata l'opzione "*Il server SMTP rifiuta la posta da indirizzi IP in lista nera*".

Sposta autom. posta lista nera in cartella spam utente
Fare clic su questa opzione per generare una cartella IMAP "Junk E-mail" per tutti i futuri account utente aggiunti a MDaemon. In questo caso, MDaemon genera automaticamente per ogni utente anche un filtro di posta che ricerca l'intestazione X-MDDNSBL-Result e sposta di conseguenza il messaggio nella cartella spam dell'utente. Facendo clic su questa opzione MDaemon richiede se si desidera o meno generare la cartella e la regola di filtro per tutti gli account utente già esistenti. Vedere *Generazione automatica della cartella Spam per ogni account*.

Generazione automatica della cartella Spam per ogni account

MDaemon è in grado di creare automaticamente una cartella di posta IMAP "Junk E-mail" per ogni account e di generare un filtro di posta per spostare i messaggi in tale cartella ogni volta che viene individuata l'intestazione `X-MDDNSBL-Result`. Quando si sceglie l'opzione *Sposta autom. posta lista nera in cartella spam utente*, si ha la possibilità di creare la cartella e i relativi filtri per tutti gli account. Per creare le cartelle e le regole, è sufficiente scegliere "sì" nella finestra di dialogo di conferma. Sebbene non sia inattaccabile, questo è un metodo agevole e generalmente affidabile per consentire agli utenti di identificare rapidamente i messaggi di posta elettronica indesiderati e di evitare che si confondano con quelli accettati. Sarà sufficiente esaminare occasionalmente il contenuto della cartella Spam solo per assicurarsi che non vi siano finiti inavvertitamente messaggi importanti, cosa che talvolta può accadere. Durante la creazione automatica delle cartelle e delle regole di filtro, se a un account è già associata una regola per il controllo dell'esistenza dell'intestazione `X-MDDNSBL-Result`, per tale account non viene intrapresa alcuna azione e non viene creata alcuna regola. Se si desidera assegnare alla cartella IMAP un nome diverso da "Junk E-mail", modificare l'impostazione predefinita dell'opzione *Nome predefinito cartella spam* situata nella schermata Sistema 194 di Impostazioni » Preferenze.

5.3.3 Honeypot spam

Con Honeypot spam (situato in Sicurezza » Spam Filter » Honeypot spam) si intendono indirizzi di e-mail locali, appositamente definiti per la raccolta della posta spam. Gli honeypot (trappole) spam non sono account o alias di indirizzi validi utilizzati per l'invio o la ricezione di posta normale. Possono essere utilizzati per inviare messaggi a newsgroup, a liste di distribuzione pubbliche o ad altre liste frequentate dagli spammer al fine di raccogliere indirizzi e-mail. In questo caso, se tutto procede come previsto, gli indirizzi honeypot spam verranno individuati dagli spammer e a essi verranno inviati messaggi spam. È inoltre possibile estrarre indirizzi di honeypot spam dai messaggi spam ricevuti e diretti a indirizzi locali non validi. Poiché gli honeypot spam non vengono utilizzati per la ricezione di posta normale, tutti i messaggi a loro indirizzati vengono sempre instradati direttamente alla cartella di apprendimento bayesiano per le successive elaborazioni. È inoltre possibile aggiungere gli indirizzi IP dei server mittenti al sistema di vaglio automatico 309, impedendo così le connessioni provenienti da tali indirizzi per un periodo di tempo specificato. Queste caratteristiche consentono di aumentare la probabilità di identificare e bloccare i messaggi spam in futuro.

Honeypot spam

Questo elenco include tutti gli indirizzi definiti come honeypot spam.

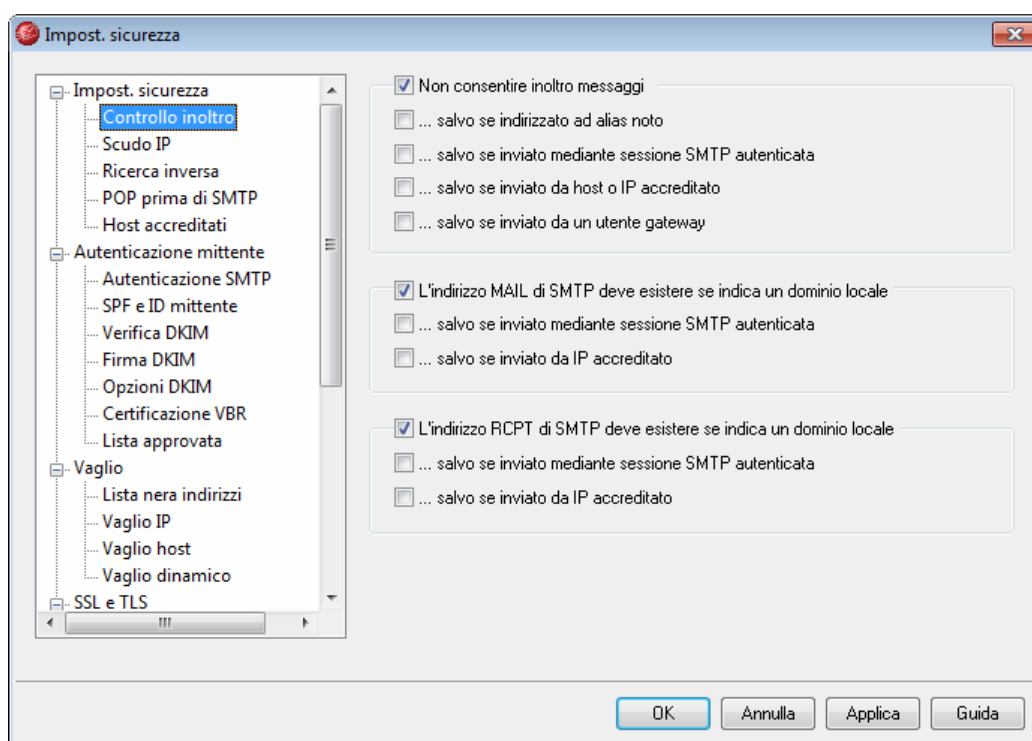
Nuovo indirizzo honeypot spam
Per aggiungere un honeypot spam, immettere l'indirizzo e fare clic su *Aggiungi*.

Rimuovi
Per rimuovere un honeypot spam, selezionare l'indirizzo desiderato e fare clic su Rimuovi.

Inoltra IP mittenti al sistema di vaglio dinamico
Selezionare questa casella di controllo se si desidera inoltrare al sistema di vaglio dinamico 309 tutti gli IP dai quali vengono inviati i messaggi honeypot spam. Per utilizzare questa funzionalità è necessario abilitare nel server la funzione di vaglio dinamico, disponibile in Sicurezza » Impostazioni sicurezza » Vaglio » Vaglio dinamico.

5.4 Impostazioni sicurezza

5.4.1 Impostazioni di sicurezza

5.4.1.1 Controllo dell'inoltro

La schermata Controllo inoltro, disponibile in Sicurezza » Impostazioni sicurezza » Controllo inoltro consente di definire il funzionamento del server per l'inoltro della posta. Quando riceve un messaggio non proveniente né destinato a un indirizzo locale, il server di posta in uso provvede a inoltrare (ossia consegnare) tale messaggio per conto di un altro server: se si preferisce non inoltrare la posta degli utenti sconosciuti, impostare i comandi descritti di seguito.

L'inoltro indiscriminato della posta per altri server può far sì che il dominio venga incluso nella lista nera di uno o più servizi DNS-BL 267. Questo tipo di inoltro aperto è caldamente sconsigliato poiché gli spammer sfruttano i server aperti per nascondere le proprie tracce.

Inoltro posta

Non consentire inoltro messaggi
Se questa opzione è selezionata, MDaemon respinge i messaggi da inoltrare in cui i mittenti (FROM) e i destinatari (TO) includano utenti non locali.

...salvo se indirizzato ad alias noto
Selezionare questa casella di controllo se si desidera che a questi alias395 vengano inoltrati messaggi, a prescindere dalle impostazioni di Controllo inoltro.

...salvo se inviato mediante sessione SMTP autenticata
Se questa opzione è abilitata, MDaemon inoltra sempre la posta, se inviata mediante una sessione SMTP autenticata.

...salvo se inviato da host o IP accreditato
Abilitare questa opzione qualora si desideri consentire l'inoltro se la posta proviene da un host o da un indirizzo IP accreditato.

...salvo se inviato da un utente gateway
Selezionare questa casella di controllo per consentire l'inoltro della posta mediante i gateway di dominio, indipendentemente dalle impostazioni di inoltro. Per impostazione predefinita, questa funzione è disabilitata (opzione consigliata).

Verifica account

L'indirizzo MAIL di SMTP deve esistere se indica un dominio locale
Selezionare questa opzione se si desidera verificare che il valore MAIL trasmesso durante il processo SMTP, se fa riferimento a un dominio o a un gateway locale, indichi un account effettivamente esistente.

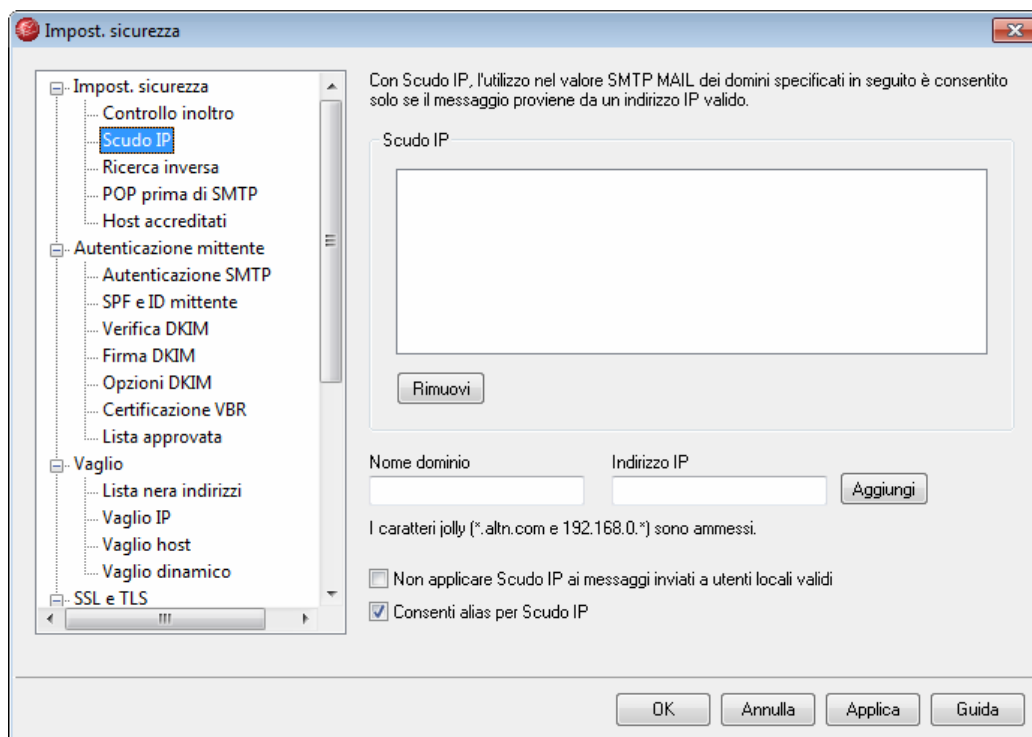
...salvo se inviato mediante sessione SMTP autenticata
Selezionare questa opzione se si desidera escludere i messaggi inviati mediante sessioni di posta SMTP autenticate dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

...salvo se inviato da host o IP accreditato
Selezionare questa opzione se si desidera escludere i messaggi inviati da un indirizzo IP accreditato dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

L'indirizzo RCPT di SMTP deve esistere se indica un dominio locale
Selezionare questa opzione se si desidera verificare che il valore RCPT trasmesso durante il processo SMTP, se fa riferimento a un dominio o a un gateway locale, indichi un account effettivamente esistente.

...salvo se inviato mediante sessione SMTP autenticata
Selezionare questa opzione se si desidera escludere i messaggi inviati mediante sessioni di posta SMTP autenticate dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere...*.

...salvo se inviato da host o IP accreditato
Selezionare questa opzione se si desidera escludere i messaggi inviati da un indirizzo IP accreditato dall'elaborazione relativa all'opzione *L'indirizzo MAIL di SMTP deve esistere....*

5.4.1.2 Scudo IP

Scudo IP, situato nel menu `Sicurezza » Impostazioni sicurezza`, è un elenco di nomi di dominio e dei corrispondenti indirizzi IP che vengono verificati durante il comando `MAIL From` impartito nella sessione SMTP. Una sessione SMTP proveniente da un utente appartenente a uno dei domini elencati viene accettata solo se proviene da uno dei relativi indirizzi IP. Ad esempio, si supponga che il nome di dominio sia mdaemon.com e che i computer della rete locale LAN usino gli indirizzi IP compresi tra 192.168.0.0 e 192.168.0.255. Con queste informazioni, Scudo IP può essere configurato per associare il nome di dominio mdaemon.com alla serie di indirizzi IP 192.168.0.* (i caratteri jolly sono consentiti). Pertanto, se un computer richiede una connessione SMTP al server, inviando l'istruzione "`MAIL FROM <someone@mdaemon.com>`", la sessione SMTP viene accettata solo se il computer che si connette presenta un indirizzo IP compreso tra 192.168.0.0 e 192.168.0.255.

È possibile escludere le sessioni autenticate dalle restrizioni dello scudo IP mediante un'opzione della schermata Autenticazione SMTP 283.

Scudo IP

Si tratta dell'elenco dei nomi di dominio e dei corrispondenti indirizzi IP che vengono confrontati quando un utente tenta di connettersi a MDaemon dichiarando di appartenere a uno di essi.

Nome dominio
Immettere il nome del dominio da associare a un intervallo di indirizzi IP specifico.

Indirizzo IP
Inserire l'indirizzo IP da associare con il nome di dominio. L'indirizzo prevede il formato con punti decimali.

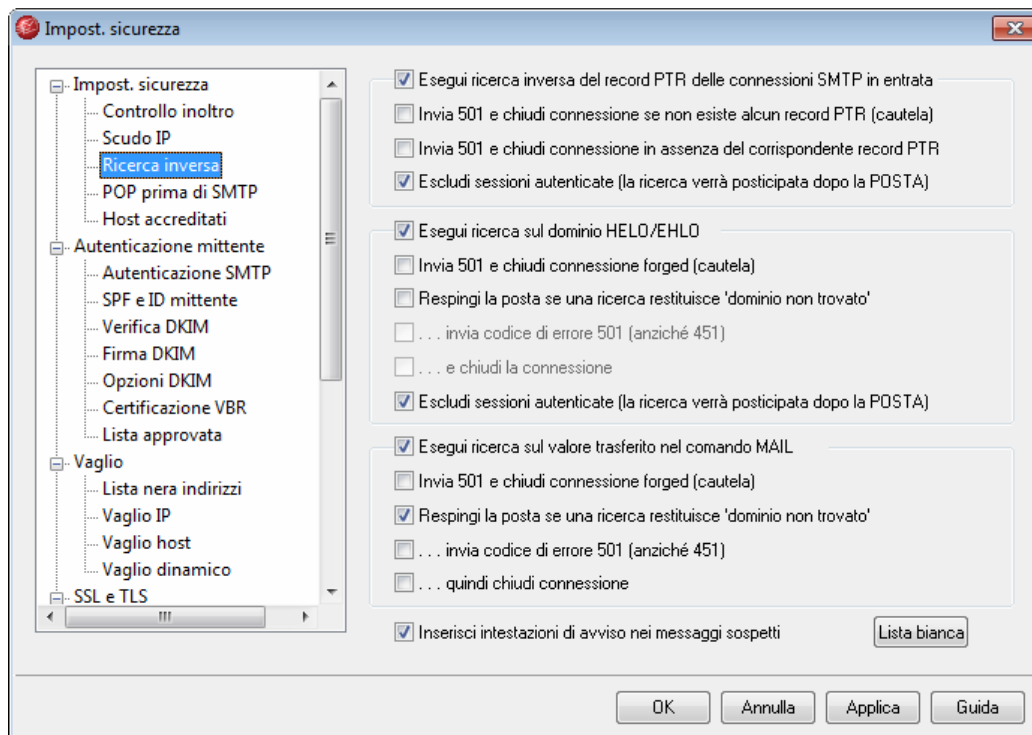
Aggiungi
Per aggiungere all'elenco l'intervallo di domini e di indirizzi IP, fare clic sul pulsante *Aggiungi*.

Rimuovi
Fare clic su questo pulsante per rimuovere le voci selezionate dall'elenco.

Non applicare Scudo IP ai messaggi inviati a utenti locali validi
Selezionare questa opzione per verificare la corrispondenza dominio/IP solo per i messaggi destinati a utenti non locali o a utenti locali non validi. In questo modo si impedisce che terzi si fingano utenti locali allo scopo di inoltrare la propria posta mediante il server e, al contempo, si risparmiano risorse in quanto non viene effettuata la verifica dei messaggi indirizzati agli utenti del server in uso. Se si seleziona sia questa opzione che l'opzione *Consenti alias per Scudo IP* descritta di seguito, verranno accettati anche i messaggi inviati ad alias validi.

Consenti alias per Scudo IP
Abilitare questa opzione se si desidera che Scudo IP accetti gli alias degli indirizzi durante la verifica dell'associazione tra domini e indirizzi IP. Con Scudo IP, l'alias viene convertito nell'account reale cui fa riferimento e, di conseguenza, viene accettato se il controllo ha esito positivo. Se questa opzione è disattivata, ogni alias viene considerato come indirizzo indipendente dall'account che rappresenta. Di conseguenza, se l'indirizzo IP di un alias viola il controllo, il messaggio viene rifiutato. Questa opzione è duplicata nella schermata Opzioni 397 di Alias e qualsiasi modifica apportata in questa sede si riflette anche sull'altra.

Se si desidera che i messaggi in entrata indirizzati ad alias validi siano esclusi dalle verifiche di Scudo IP, abilitare sia questa opzione che l'opzione *Non applicare Scudo IP ai messaggi inviati a utenti locali validi*.

5.4.1.3 Ricerca inversa

Le opzioni di questa schermata consentono di configurare MDaemon in modo da eseguire una ricerca inversa sul dominio trasmesso nei comandi `HELO/EHLO` e `MAIL`. Durante le ricerche, MDaemon tenta di acquisire tutti gli indirizzi IP dei record MX e A per il dominio specifico; successivamente, l'indirizzo IP del computer che richiede la connessione viene confrontato con l'elenco allo scopo di determinare l'esatta identità del mittente.

Spesso l'indirizzo IP di un server che invia posta non corrisponde ad alcun record MX o A conosciuto per un dato dominio, senza che ciò impedisca al server di inviare posta in maniera legittima. Lo scopo della ricerca inversa non è dunque quello di escludere posta, ma di includere il maggior numero di informazioni nei file di registro e di fornire i mezzi necessari ai postmaster per intervenire a seconda dei criteri di protezione locali nei confronti dei messaggi sospetti. A tale scopo, esiste un'opzione che consente di inserire un'intestazione speciale in tutti i messaggi che non passano al vaglio di una ricerca inversa: i messaggi contenenti tale intestazione verranno quindi gestiti in base a quanto specificato nella funzione Filtro contenuti.

La ricerca inversa può inoltre essere eseguita sui record PTR (puntatore) degli indirizzi IP in entrata: mediante questa opzione, se l'indirizzo IP in entrata non corrisponde ad alcun record PTR, è possibile interrompere la connessione o inserire un'intestazione di avviso nel messaggio.

È opinione comune che l'accettazione di posta proveniente da utenti che si identificano mediante un dominio inesistente debba essere facoltativa: a tale scopo, è disponibile un comando per rifiutare i messaggi per i quali la ricerca inversa restituisce un messaggio "dominio non trovato", proveniente dal server DNS. In questi casi, MDaemon restituisce il codice di errore `451`, respinge il messaggio e consente il proseguimento

della sessione SMTP. Tuttavia, è possibile inviare il codice di errore `501`, chiudere la connessione socket oppure eseguire entrambe le operazioni. A tale scopo sono disponibili ulteriori comandi.

Gli indirizzi IP e l'host locale (127.0.0.1) accreditati sono sempre esclusi dalle ricerche inverse.

Esegui ricerca inversa del record PTR delle connessioni SMTP in entrata
Selezionare questa opzione per effettuare la ricerca del record PTR in tutte le connessioni SMTP in entrata.

Invia 501 e chiudi connessione se non esiste alcun record PTR (cautela)
Se questa casella di controllo è selezionata, MDaemon invia il codice di errore `501`, che indica un errore di sintassi relativo ai parametri o agli argomenti, e chiude la connessione qualora non venga trovato alcun record PTR relativo al dominio.

Invia 501 e chiudi connessione in assenza del corrispondente record PTR
Se questa casella di controllo è selezionata, MDaemon invia il codice di errore `501`, che indica un errore di sintassi relativo ai parametri o agli argomenti, e chiude la connessione qualora la ricerca del record PTR non restituisca alcuna corrispondenza.

Escludi sessioni autenticate (la ricerca verrà differita fino a MAIL)
Selezionare questa opzione se si desidera differire la ricerca PTR per le connessioni SMTP in entrata fino all'invio del comando MAIL del protocollo SMTP, utilizzato per verificare se la connessione è autenticata o meno.

Esegui ricerca sul dominio HELO/EHLO
Selezionare questa casella di controllo per eseguire una ricerca sul nome di dominio riportato durante la parte `HELO/EHLO` della sessione. Il comando `HELO/EHLO` viene utilizzato dal client (computer mittente) per identificarsi presso il server. Il nome di dominio trasmesso dal client in questo comando viene inserito dal server nella sezione `From` dell'intestazione `Received`.

Esegui ricerca sul valore trasferito nel comando MAIL
Se questa opzione è abilitata, la ricerca viene effettuata sul nome di dominio trasmesso durante la parte relativa al comando `MAIL` della transazione di posta. L'indirizzo trasmesso nel comando `MAIL` coincide generalmente con l'indirizzo del mittente, cioè con la casella postale da cui è partito il messaggio; tuttavia, a volte può trattarsi dell'indirizzo a cui devono essere inviati i messaggi di errore.

Invia 501 e chiudi connessione forged (cautela)
Selezionare questa casella di controllo se si desidera inviare il codice di errore 501 e chiudere la connessione quando dalla ricerca risulta un'identificazione contraffatta.

Spesso il risultato della ricerca inversa che rileva un'identificazione contraffatta non è corretto; è molto frequente, infatti, che i server di posta identifichino se stessi con valori che non corrispondono ai relativi indirizzi IP. Ciò può dipendere da restrizioni e limiti ISP oltre ad altre possibili cause. Per questo motivo è opportuno prestare la massima attenzione prima di attivare questa opzione in quanto il server potrebbe respingere posta accettabile.

Respingi la posta se una ricerca restituisce 'dominio non trovato'
Attivando questa opzione, nel caso in cui la ricerca restituisca come risultato "dominio non trovato", il messaggio viene respinto con il codice di errore 451 (Azione richiesta interrotta: errore locale di elaborazione), quindi la sessione prosegue e si conclude normalmente.

...invia codice di errore 501 (anziché 451)
Selezionare questa casella di controllo per inviare in risposta al risultato "dominio non trovato" il codice di errore 501, che indica un errore di sintassi relativo ai parametri o agli argomenti, anziché il codice di errore 451.

...quindi chiudi connessione
Selezionare questa casella di controllo per chiudere immediatamente la connessione, anziché consentirne il proseguimento, se la ricerca inversa restituisce il risultato "dominio non trovato".

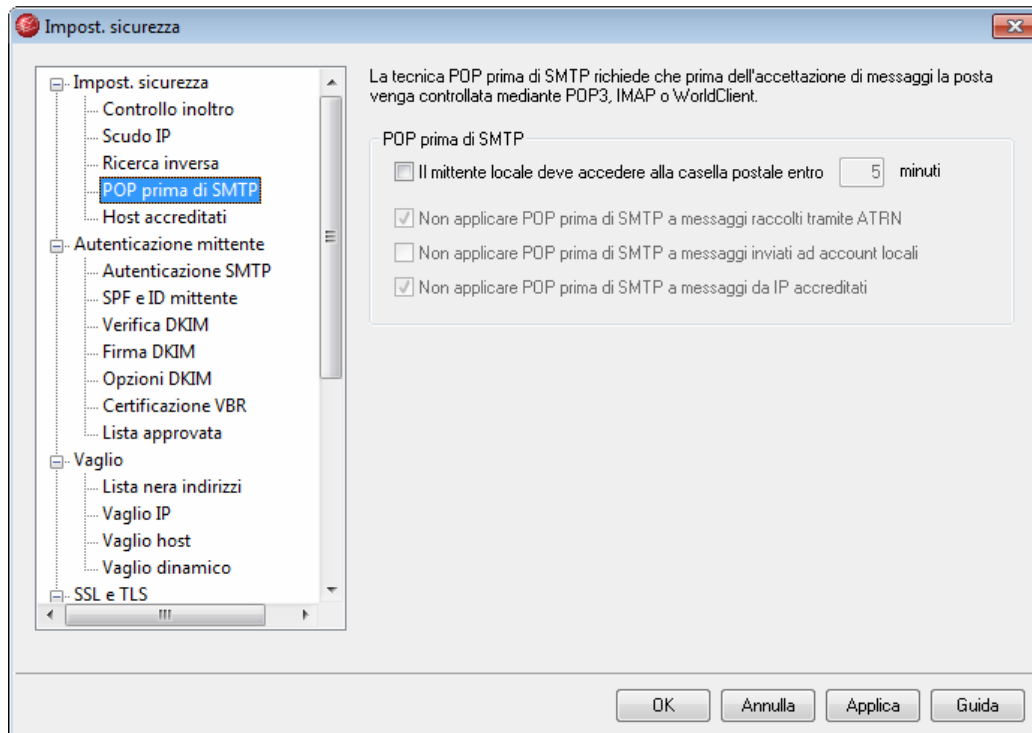
Sessioni autenticate esenti (ricerca differita fino a MAIL)
Selezionare questa opzione se si desidera differire la ricerca fino all'invio del comando MAIL del protocollo SMTP al fine di verificare se la connessione utilizzerà l'autenticazione o meno.

Inserisci intestazioni di avviso nei messaggi sospetti
Selezionare questa casella di controllo per inserire un'intestazione nei messaggi considerati sospetti al termine di una ricerca inversa. Per modificare il nome e il contenuto dell'intestazione, modificare la chiave seguente del file MDaemon.ini:

```
[Special]
LookupWarningHeader=X-Lookup-Warning: testo
```

MDaemon non pone limiti alla modifica della sezione "X-LookupWarning: testo", a patto che sia conforme alle norme RFC relative alle intestazioni di posta.

Lista bianca
Fare clic su questo pulsante per aprire la finestra di dialogo Lista bianca all'interno della quale inserire gli indirizzi IP, i domini e gli host che si desidera escludere dalla funzione di ricerca inversa.

5.4.1.4 POP prima di SMTP

POP prima di SMTP

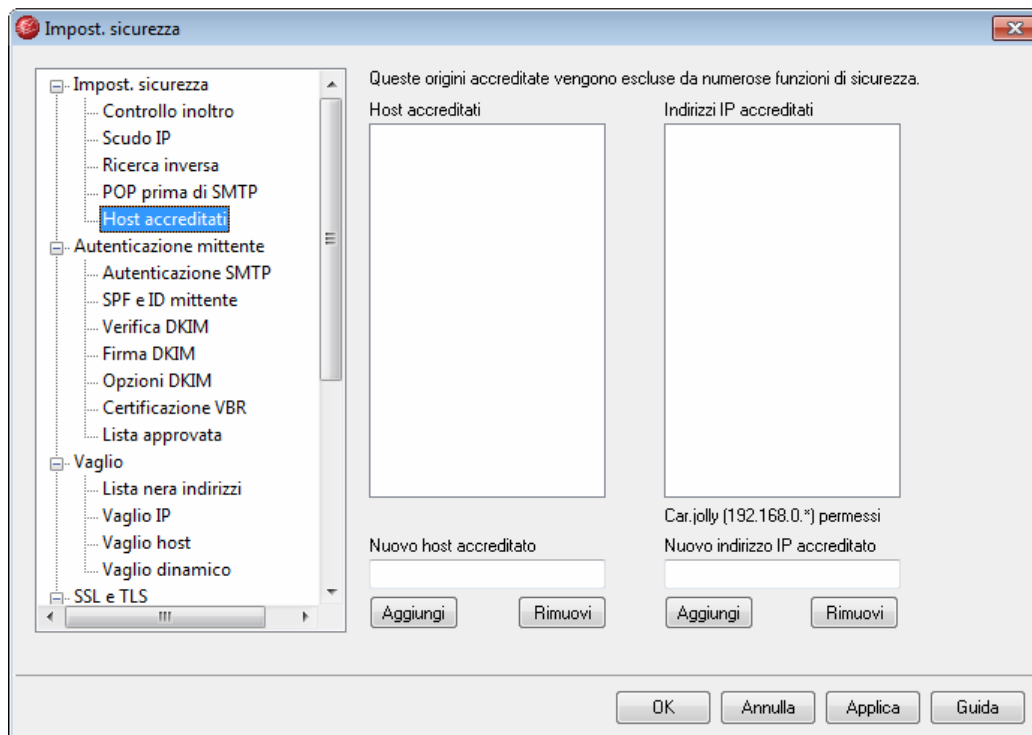
Il mittente locale deve accedere alla casella postale entro [XX] minuti
Se questa funzionalità è abilitata, per inviare messaggi di posta provenienti da mittenti locali è necessario che l'utente locale si connetta e controlli la propria casella postale entro l'intervallo di tempo, espresso in minuti, specificato in questo campo.

Non applicare POP prima di SMTP a messaggi raccolti tramite ATRN
Selezionare questa casella di controllo per non applicare ai messaggi raccolti mediante ATRN467 la funzionalità POP prima di SMTP.

Non applicare POP prima di SMTP a messaggi inviati ad account locali
Fare clic su questa casella di controllo per non applicare la funzionalità POP prima di SMTP ai messaggi inviati da un utente locale a un altro. In genere, MDaemon applica la funzione POP prima di SMTP non appena riconosce il mittente ma, se questa opzione è abilitata, MDaemon procede al riconoscimento del destinatario del messaggio prima di determinare se tale funzionalità debba essere applicata o meno.

Non applicare POP prima di SMTP a messaggi da IP accreditati
Se questa casella di controllo è abilitata, i messaggi provenienti da un indirizzo IP elencato nella schermata Host accreditati282 vengono esclusi dalla funzionalità POP prima di SMTP.

Per non applicare la funzionalità POP prima di SMTP alle sessioni autenticate è possibile utilizzare un'opzione della schermata Autenticazione SMTP 283.

5.4.1.5 Host accreditati

Numerose finestre di dialogo e funzioni di sicurezza di MDaemon includono opzioni che consentono di scegliere se escludere o meno dall'elaborazione gli "host accreditati", i "domini accreditati" o gli "indirizzi IP accreditati". Tali opzioni fanno riferimento agli host e agli indirizzi IP visualizzati in questa schermata.

Host accreditati
Viene visualizzato un elenco degli host esclusi da specifiche opzioni di sicurezza.

Nuovo host accreditato
Inserire il nome di un dominio da aggiungere all'elenco degli *host accreditati*.

Aggiungi
Fare clic su questo pulsante per aggiungere il nuovo dominio all'elenco degli *host accreditati*.

Rimuovi
Fare clic su questo pulsante per rimuovere le voci selezionate dall'elenco degli *host accreditati*.

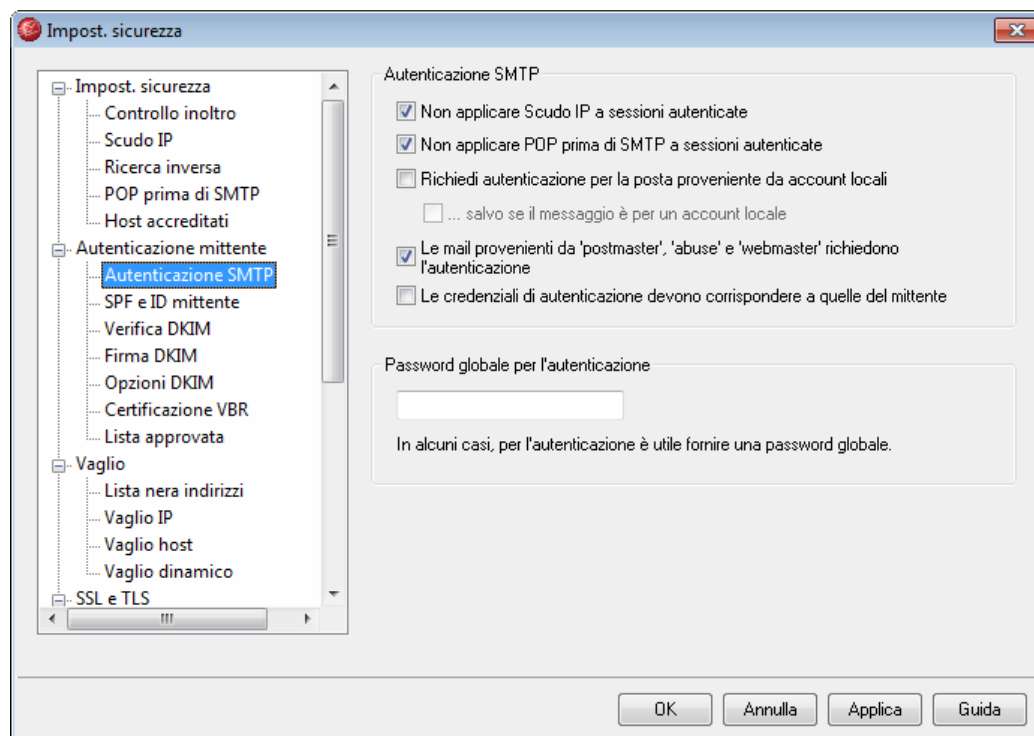
Indirizzi IP accreditati
Viene visualizzato un elenco degli indirizzi IP esclusi da specifiche opzioni di sicurezza.

Nuovo indirizzo IP accreditato
Inserire l'indirizzo IP da aggiungere all'elenco degli *Indirizzi IP accreditati*.

Aggiungi
Fare clic su questo pulsante per aggiungere il nuovo indirizzo IP all'elenco degli *Indirizzi IP accreditati*.

Rimuovi
Fare clic su questo pulsante per rimuovere le voci selezionate dall'elenco degli *Indirizzi IP accreditati*.

5.4.2 Autenticazione mittente

5.4.2.1 Autenticazione SMTP

Autenticazione SMTP

Non applicare Scudo IP a sessioni autenticate
Con l'attivazione di questo controllo, gli utenti autenticati vengono esclusi dalle restrizioni di Scudo IP 276. La posta proveniente da questi utenti viene accettata a prescindere dall'indirizzo IP di connessione.

Non applicare POP prima di SMTP a sessioni autenticate
Se si è abilitata la funzione di sicurezza POP prima di SMTP[281], è sufficiente fare clic su questa opzione per escludere gli utenti autenticati da questa restrizione. In questo modo, non è necessario che un utente autenticato esegua una verifica della posta prima dell'invio.

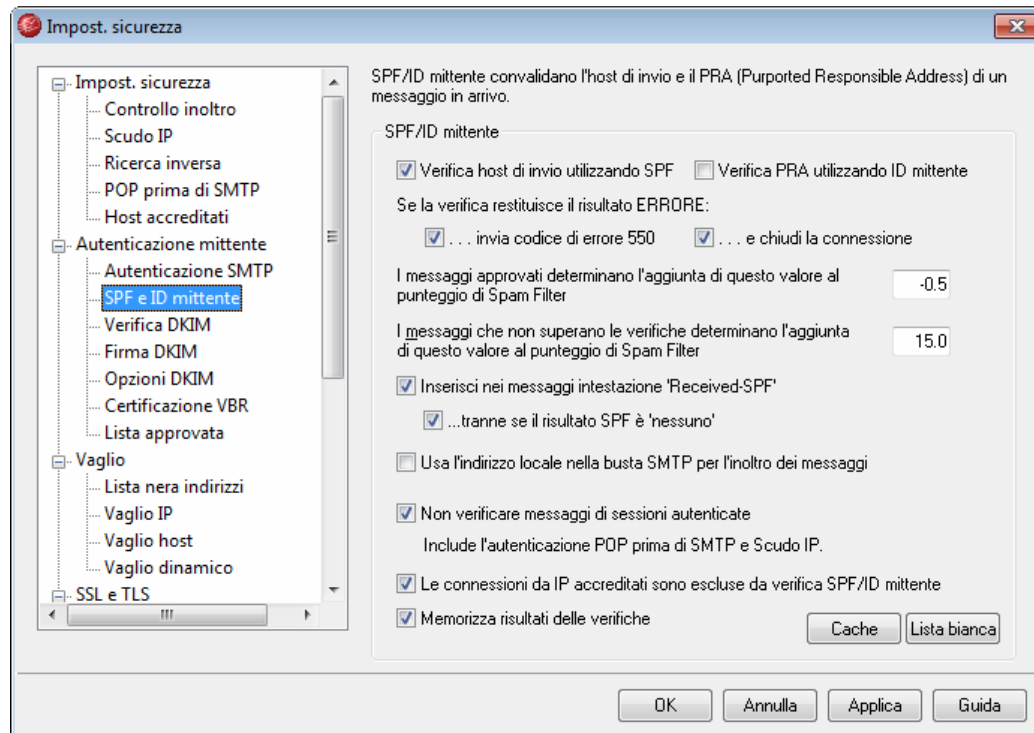
Richiedi autenticazione per la posta proveniente da account locali
Se questa opzione è abilitata e il messaggio in arrivo sembra provenire da uno dei domini di MDaemon, per evitare che MDaemon rifiuti la consegna del messaggio l'account deve essere preventivamente autenticato.

...salvo se il messaggio è per un account locale
Se l'autenticazione dei messaggi provenienti da un mittente locale è obbligatoria, selezionare questa opzione per evitare la restrizione relativa all'autenticazione quando anche il destinatario è locale. Nota: in alcuni casi questa funzione risulta necessaria, ad esempio quando si richiede agli utenti l'uso di server di posta differenti per i messaggi in entrata e quelli in uscita.

Le mail provenienti da 'postmaster', 'abuse' e 'webmaster' richiedono l'autenticazione
Selezionare questa casella di controllo per richiedere l'autenticazione dei messaggi che dichiarano di provenire dagli alias o dagli account "postmaster@...", "abuse@..." o "webmaster@..." prima dell'accettazione da parte di MDaemon. Spammer e hacker sono a conoscenza della potenziale esistenza di tali indirizzi e possono, quindi, tentare di utilizzarli per inviare posta attraverso il sistema. Questa opzione consente di evitare questa eventualità. Questa opzione è duplicata nella schermata Opzioni[397] di Alias. Qualsiasi modifica apportata in questa sede viene riportata anche nell'altra posizione.

Le credenziali di autenticazione devono corrispondere a quelle del mittente
Questa opzione consente di richiedere che il mittente utilizzi per l'autenticazione solo le proprie credenziali. Così, ad esempio, *franco@esempio.com* potrà essere autenticato solo mediante le credenziali dell'account *franco@esempio.com*. Il tentativo di autenticazione mediante *franco02@esempio.com* verrà respinto anche se le credenziali di *franco02@esempio.com* sono valide. L'opzione è disabilitata per impostazione predefinita.

Password globale per l'autenticazione
Per alcune configurazioni può essere necessaria una password globale per l'autenticazione. Se lo si desidera, indicarla in questo campo.

5.4.2.2 SPF e ID mittente

MDaemon supporta le infrastrutture SPF (Sender Policy Framework) e SIDF (Sender ID Framework) che consentono la verifica dei server di invio e la protezione da spoofing e phishing, due tipi di contraffazione della posta elettronica con cui il mittente tenta di far apparire i messaggi come inviati da qualcun altro.

Molti domini pubblicano i record MX nel DNS (Domain Name System) per identificare le postazioni a cui è consentito ricevere la posta elettronica, ma ciò non consente di identificare in alcun modo le postazioni a cui è consentito *inviare* la posta. SPF è un mezzo attraverso il quale i domini possono pubblicare anche i record relativi ai mittenti per identificare le postazioni autorizzate all'invio dei messaggi. Eseguendo una ricerca SPF sui messaggi in entrata, MDaemon può tentare di determinare se al server di invio è consentito consegnare la posta relativa al dominio di invio dichiarato e, di conseguenza, se l'indirizzo del mittente può essere stato contraffatto o "mascherato". La tecnologia ID mittente è correlata a SPF, ma è più complessa e consente di determinare in modo più affidabile il dominio effettivamente responsabile dell'invio del messaggio e di ridurre la probabilità di risultati errati.

Le opzioni di questa scheda consentono di configurare le impostazioni relative alle infrastrutture SPF e ID mittente del server.

Per ulteriori informazioni su SPF, vedere:

http://spf.pobox.com.

Per ulteriori informazioni su ID mittente, vedere:

http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

SPF/ID mittente

Verifica host di invio utilizzando SPF
Selezionando questa casella di controllo, MDaemon eseguirà interrogazioni relative ai dati SPF nell'host di invio di qualunque messaggio in entrata non proveniente da indirizzi IP contenuti nelle liste bianche o da sessioni escluse dall'elaborazione quali le connessioni autenticate o gli indirizzi IP accreditati (se queste esclusioni sono state precedentemente abilitate). L'host di cui MDaemon esegue la verifica viene ricavato dal valore `MAIL` trasferito durante l'elaborazione SMTP. Questa opzione di verifica SPF è attivata per impostazione predefinita.

Verifica PRA utilizzando ID mittente
Attivare questa opzione se si desidera utilizzare l'infrastruttura SIDF (Sender ID Framework) per verificare i messaggi in entrata. MDaemon identifica il PRA (Purported Responsible Address) del messaggio in arrivo tramite un'ispezione accurata delle intestazioni e quindi verifica se il messaggio arriva da tale posizione. Il PRA è il più recente indirizzo ritenuto responsabile dell'invio del messaggio, che non corrisponde necessariamente al mittente originale.

Se la verifica restituisce il risultato ERRORE:

...invia codice di errore 550
Selezionare questa casella di controllo per inviare il codice di errore 550 quando il risultato dell'interrogazione SPF /ID mittente è "Fail".

...quindi chiudi connessione
Attivare questa opzione per chiudere la connessione subito dopo l'invio del codice di errore 550.

I messaggi approvati determinano l'aggiunta di questo valore al punteggio di Spam Filter
Indicare il valore che si desidera aggiungere al punteggio di spam del messaggio quando SPF/ID mittente conferma che esso proviene da un dominio situato nell' elenco approvato 303.

In genere, il valore specificato in questo campo deve essere un numero negativo in modo da diminuire il punteggio di spam per i messaggi approvati.

I messaggi che non superano la verifica SPF determinano l'aggiunta di questo valore al punteggio di Spam Filter
Indicare il valore da aggiungere al punteggio di spam del messaggio quando esso non supera la verifica SPF/ID mittente.

Inserisci nei messaggi intestazione 'Received-SPF'
Selezionare questa opzione per inserire in ciascun messaggio un'intestazione "Received-SPF".

...tranne se il risultato SPF è 'nessuno'
Attivare questa opzione per non inserire nel messaggio l'intestazione "Received-

SPF" quando il risultato dell'interrogazione SPF è "nessuno".

Usa l'indirizzo locale nella busta SMTP per l'inoltro dei messaggi
Scegliere questa opzione se si desidera che tutta la posta inoltrata da MDaemon utilizzi un indirizzo locale nella busta SMTP. Ciò consente di ridurre i problemi associati all'inoltro della posta. In genere, i messaggi inoltrati vengono inviati utilizzando l'indirizzo di posta del mittente originale e non quello di chi esegue l'inoltro. In alcuni casi, l'uso di un indirizzo locale si rivela necessario per impedire al server ricevente di interpretare erroneamente il messaggio inoltrato come contraffatto tramite "spoofing".

Opzioni di verifica

Non verificare messaggi di sessioni autenticate
Selezionare questa casella di controllo per escludere le connessioni autenticate dalle interrogazioni SPF/ID mittente. Le sessioni autenticate includono quelle verificate mediante l'autenticazione SMTP283, POP prima di SMTP281 o Scudo IP276..

Le connessioni da IP accreditati sono escluse da verifica SPF/ID mittente
Attivare questa opzione per escludere dalla verifica SPF/ID mittente le connessioni da indirizzi IP accreditati282.

Memorizza risultati delle verifiche
Selezionare questa opzione per memorizzare temporaneamente nella cache i risultati delle interrogazioni SPF.

Cache
Questo pulsante apre la cache di SPF.

Lista bianca
Fare clic su questo pulsante per aprire la lista bianca di SPF, nella quale è possibile inserire gli indirizzi IP che si desidera escludere dalle ricerche SPF.

5.4.2.3 DomainKeys Identified Mail (DKIM)

DomainKeys (DK) e DomainKeys Identified Mail (DKIM) sono sistemi crittografici di verifica della posta elettronica che possono essere utilizzati per impedire lo "spoofing", ovvero la pratica del contraffare l'indirizzo e-mail di un altro utente fingendosi un mittente diverso. Inoltre, poiché numerosi messaggi spam contengono indirizzi contraffatti, le tecnologie DK e DKIM consentono di ridurne significativamente il numero, pur non essendo nate come strumenti antispam. Le tecnologie DK/DKIM possono essere utilizzate per garantire l'integrità dei messaggi in arrivo o per assicurarsi che il messaggio non sia stato alterato nell'intervallo di tempo trascorso dal momento in cui ha lasciato il server di posta del firmatario al momento in cui è arrivato a destinazione. In altre parole, grazie alla verifica crittografica di DK e DKIM, il server ha la certezza di ricevere il messaggio dal server che lo ha firmato e la garanzia che nessun altro lo abbia in alcun modo alterato.

Per garantire la validità e l'integrità dei messaggi, la tecnologia DK/DKIM si avvale di un

sistema di coppie di chiavi pubbliche e private. Sui record DNS del server di invio viene pubblicata una chiave pubblica crittografata, quindi ciascun messaggio in uscita viene firmato dal server usando la corrispondente chiave privata crittografata. Per i messaggi in arrivo, quando il server ricevente rileva la firma del messaggio, recupera la chiave pubblica dai record DNS del server di invio, quindi confronta la chiave con la firma crittografata del messaggio per determinarne la validità. Se il server ricevente non riesce a verificare il messaggio in arrivo, ciò vuol dire che contiene un indirizzo contraffatto oppure che è stato alterato o modificato. Il messaggio bloccato viene quindi respinto oppure accettato ma associato a un punteggio di spam.

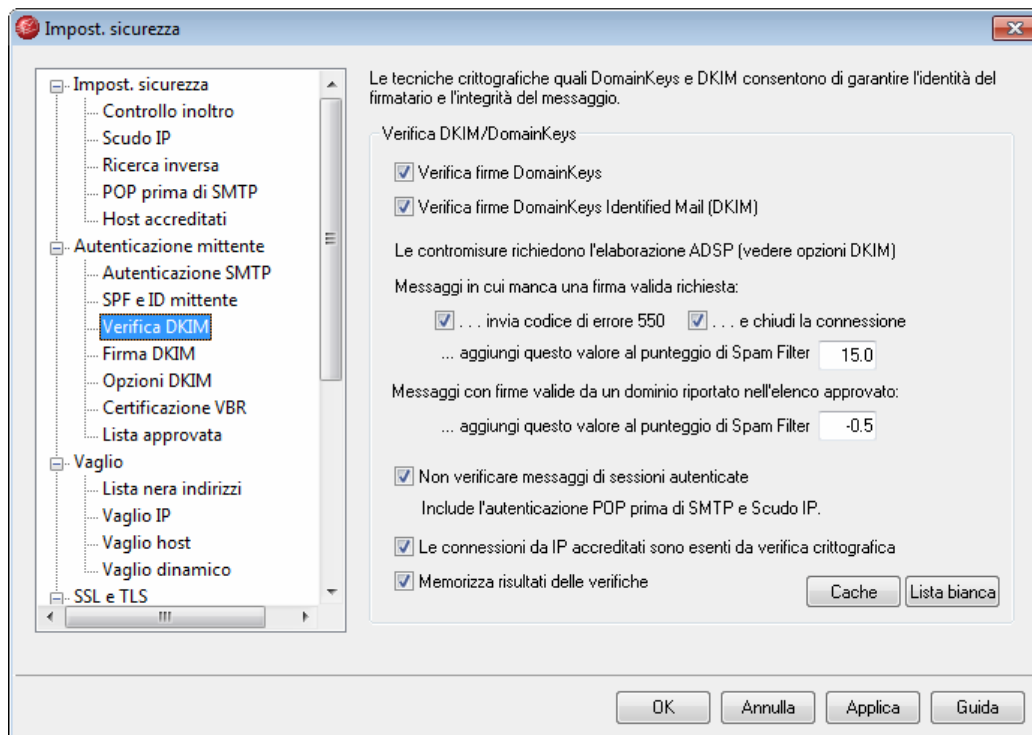
Per configurare MDaemon al fine di verificare la firma crittografica dei messaggi in arrivo, utilizzare le opzioni incluse nella schermata Verifica DKIM289. Per configurare MDaemon al fine di firmare i messaggi in uscita, utilizzare le opzioni incluse nella schermata Firma DKIM293. Entrambe le schermate si trovano nella sezione Autenticazione mittente della finestra di dialogo Impostazioni sicurezza, disponibile in: Sicurezza » Impostazioni sicurezza » Autenticazione mittente. L'interfaccia principale28 di MDaemon contiene la scheda DK/DKIM, all'interno della scheda Sicurezza, che consente di monitorare l'attività in tempo reale di DK/DKIM. Per registrare tale attività, utilizzare le opzioni disponibili in: Impostazioni» Dominio predefinito/server » Registrazione » Opzioni.

Vedere:

Verifica DKIM 289
Firma DKIM 293
Opzioni DKIM 296

Per ulteriori informazioni su DomainKeys Identified Mail, visitare il sito http://www.dkim.org/.

Per ulteriori informazioni su DomainKeys, visitare il sito http://antispam.yahoo.com/domainkeys.

5.4.2.3.1 Verifica DKIM

In questa schermata è possibile configurare MDaemon affinché verifichi le firme DomainKeys Identified Mail (DKIM) e/o DomainKeys (DK) nei messaggi remoti in arrivo. Se si utilizza questa funzionalità e un messaggio in arrivo contiene una firma crittografata, MDaemon rileva la chiave pubblica dal record DNS del dominio individuato mediante la firma e utilizza la chiave per determinare la validità della firma DK o DKIM del messaggio.

Se la verifica della firma ha esito positivo, l'elaborazione del messaggio passa alla fase successiva del normale processo di consegna. Se il dominio individuato mediante la firma è presente anche nell'elenco approvato 303, inoltre, il punteggio spam del messaggio viene corretto in senso positivo.

Se un messaggio è privo di firma o se quest'ultima non è valida, MDaemon recupera il record ADSP (Author Domain Signing Practices) del dominio dall'intestazione `From` per verificare se i messaggi relativi a tale dominio debbano o meno essere firmati. Se il record ADSP indica che la firma è richiesta e se la chiave pubblica indica che chi appone la firma non sta semplicemente collaudando la funzionalità DKIM, la verifica del messaggio ha esito negativo e il messaggio viene elaborato in base a tale risultato: può essere respinto direttamente oppure accettato, con un conseguente incremento del punteggio spam.

Infine, se per un record ADSP del sito viene utilizzata una sintassi sconosciuta a MDaemon, se il record non esiste affatto o se l'opzione ADSP della schermata Opzioni DKIM 296 è disabilitata, non verranno prese contromisure. I messaggi non firmati o con firma non valida verranno considerati come provenienti da un dominio che firma solo alcuni dei messaggi.

Per ulteriori informazioni su DKIM, vedere: http://www.dkim.org/

Verifica DKIM/DomainKeys

Verifica firme DomainKeys
Per attivare la verifica DomainKeys sui messaggi remoti in arrivo, selezionare questa opzione.

Verifica firme DomainKeys Identified Mail (DKIM)
Per attivare la verifica DomainKeys Identified Mail sui messaggi remoti in arrivo, selezionare questa opzione. Quando MDaemon è stato configurato per la verifica delle firme sia DKIM che DK e un messaggio include entrambi i tipi di firma, se la verifica della firma DKIM ha esito positivo le verifiche DK non hanno luogo. Questa opzione è necessaria se si è installato SecurityPlus per MDaemon e si desidera utilizzarne la funzione Aggiornamenti urgenti163.

Risultati della verifica

Messaggi in cui manca una firma valida richiesta:
Le contromisure disponibili possono essere applicate ai messaggi solo se è stata abilitata l'opzione ADSP (Author Domain Signing Practices) della schermata Opzioni DKIM296. Se l'opzione ADSP è disabilitata, i messaggi non vengono respinti e non ottengono un punteggio spam negativo con la verifica DKIM, indipendentemente da queste impostazioni.

...invia codice di errore 550
Se il record ADSP indica che è necessaria una firma valida, tutti i messaggi che ne sono privi vengono respinti. MDaemon restituirà il codice di errore 550, respingendo il messaggio durante il processo SMTP. Se, tuttavia, la chiave pubblica di chi appone la firma indica che si tratta di un semplice collaudo della funzionalità DK/DKIM, il messaggio viene elaborato normalmente.

...e chiudi la connessione
Selezionare questa opzione se si desidera chiudere la connessione con il server mittente qualora un messaggio venga respinto in base all'opzione precedente. Se questa opzione non è selezionata, il messaggio viene ugualmente respinto in base all'opzione precedente, ma la connessione non viene chiusa.

...aggiungi questo valore al punteggio di Spam Filter
Se il record ADSP indica che è necessaria una firma valida, al punteggio di Spam Filter dei messaggi che ne sono privi verrà aggiunto questo valore. Se, tuttavia, è stata abilitata l'opzione "*...invia codice di errore*", il messaggio verrà respinto come non valido senza essere elaborato da Spam Filter. In ogni caso, se la chiave pubblica del firmatario indica che nel dominio è in corso l'esecuzione della verifica, non verrà intrapresa alcuna azione e il punteggio di Spam Filter non verrà modificato.

Se si utilizza questa opzione, è comunque possibile che alcuni messaggi vengano respinti se il punteggio spam risultante supera la soglia SMTP indicata nella schermata Spam Filter244.

Messaggi con firme valide da un dominio riportato nell'elenco approvato:

...aggiungi questo valore al punteggio di Spam Filter
Se il dominio individuato tramite la firma si trova nell'elenco approvato[303], il valore indicato in questo campo viene aggiunto al punteggio spam di ogni messaggio firmato mediante DK o DKIM che supera la verifica. Quando la firma di un messaggio viene verificata, ma il dominio non si trova nell'elenco approvato, il punteggio spam non viene modificato e il superamento della verifica non incide sul punteggio. Tuttavia, al messaggio continuano ad essere applicati l'elaborazione e il punteggio normali di Spam Filter.

In genere, il valore specificato in questo campo deve essere un numero negativo in modo da diminuire il punteggio di spam per i messaggi contenenti firme crittografiche valide quando il dominio individuato mediante la firma si trova nell'elenco approvato[303]. Il valore predefinito per questa opzione è `-0.5`.

Opzioni di verifica

Non verificare messaggi di sessioni autenticate
Questa opzione consente di escludere i messaggi dalla verifica crittografica quando la sessione è autenticata. Le sessioni autenticate includono quelle verificate mediante autenticazione SMTP[283], POP prima di SMTP[281] o Scudo IP[276].

Le connessioni da IP accreditati sono esenti da verifica crittografica
Questa opzione consente di escludere dalla verifica crittografica le connessioni provenienti da indirizzi IP accreditati[282].

Memorizza risultati delle verifiche
Selezionare questa opzione se si desidera memorizzare nella cache le informazioni DK/DKIM rilevate durante la ricerca DNS. Memorizzando momentaneamente nella cache le informazioni contenute in un record DNS del dominio, è possibile aumentare l'efficienza di elaborazione dei successivi messaggi DK/DKIM firmati, provenienti dallo stesso dominio.

Cache
Questo pulsante apre il file della cache di DomainKeys. Se si utilizza l'opzione *Memorizza risultati delle verifiche* descritta precedentemente, nel file vengono elencate tutte le informazioni archiviate nella cache.

Lista bianca
Questo pulsante consente di aprire l'elenco delle eccezioni. I messaggi provenienti da un qualsiasi indirizzo IP presente in questo elenco non sono soggetti a verifica crittografica.

Intestazione "Authentication-Results"

Ogni volta che un messaggio viene autenticato tramite verifica SMTP AUTH, SPF, DomainKeys o DomainKeys Identified Mail, MDaemon inserisce nel messaggio l'intestazione "Authentication-Results" elencando i risultati del processo di

autenticazione. Se MDaemon è configurato in modo da accettare anche i messaggi che non superano l'autenticazione, l'intestazione "Authentication-Results" contiene un codice indicante la causa dell'errore.

L'IETF (Internet Engineering Task Force) è attualmente impegnata a modificare alcuni standard relativi a questa intestazione e ai protocolli citati in questa sezione. Per ulteriori informazioni consultare il sito Web IETF all'indirizzo: http://www.ietf.org/.

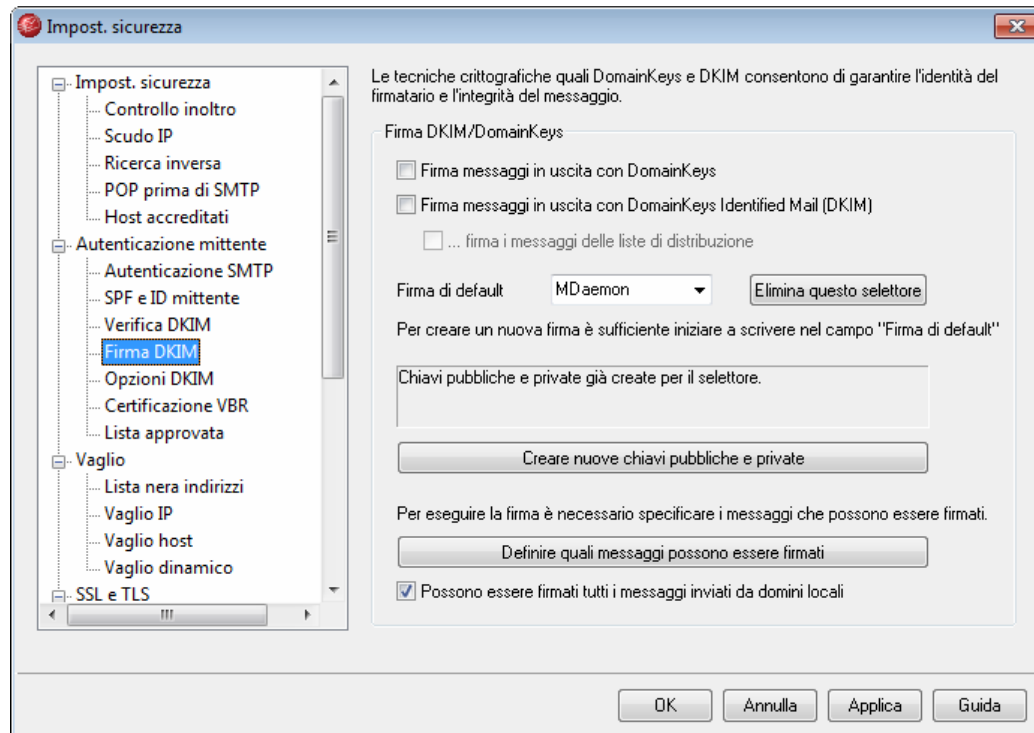
Intestazioni DK/DKIM nei messaggi delle liste di distribuzione

Per impostazione predefinita, MDaemon rimuove le firme DK/DKIM dai messaggi delle liste in arrivo poiché le firme potrebbero essere danneggiate a causa delle modifiche apportate alle intestazioni o ai contenuti dei messaggi durante l'elaborazione delle liste. Se si desidera che MDaemon lasci le firme nei messaggi di una lista, è possibile configurarlo manualmente impostando la seguente opzione nel file `MDaemon.ini`:

```
[DomainKeys]
StripSigsFromListMail=No (il valore predefinito è "Yes")
```

Per ulteriori informazioni, vedere:

DomainKeys Identified Mail (DKIM) 287
Firma DKIM 293
Opzioni DKIM 296

5.4.2.3.2 Firma DKIM

Utilizzare le opzioni incluse nella scheda Firma DKIM per verificare e stabilire a quali messaggi in uscita debba essere applicata una firma crittografica, nonché il metodo utilizzato per la firma (DK e/o DKIM). È possibile, inoltre, utilizzare questa finestra per indicare i selettori e generare le chiavi pubbliche e private corrispondenti, compatibili con la specifica DK e DKIM. All'avvio vengono creati automaticamente i valori predefiniti relativi al selettore ("MDaemon"), alla chiave pubblica e alla chiave privata. Tutte le chiavi sono univoche e diverse da un sito all'altro, indipendentemente dal selettore specificato. Per impostazione predefinita, le chiavi vengono generate con una profondità di 1024 bit.

Firma DKIM/DomainKeys

Firma messaggi in uscita con DomainKeys
Selezionare questa opzione se si desidera applicare ad alcuni messaggi in uscita una firma crittografica utilizzando DomainKeys. Perché venga firmato, un messaggio deve soddisfare i criteri specificati in *Definire quali messaggi possono essere firmati* e deve essere ricevuto da MDaemon per la consegna in una sessione autenticata. Questa azione corrisponde all'opzione "*Firma con il selettore DomainKeys*" di Filtro contenuti utilizzata per firmare i messaggi.

Firma messaggi in uscita con DomainKeys Identified Mail (DKIM)
Selezionare questa opzione se si desidera applicare ad alcuni messaggi in uscita una firma crittografica utilizzando DomainKeys Identified Mail. Perché venga firmato, un messaggio deve soddisfare i criteri specificati in *Definire quali messaggi possono essere firmati* e deve essere ricevuto da MDaemon per la consegna in una sessione autenticata. Questa azione corrisponde all'opzione "*Firma con il selettore DKIM*" di Filtro contenuti usata per firmare i messaggi.

...firma i messaggi delle liste di distribuzione
Selezionare questa casella di controllo se si desidera applicare una firma crittografica a tutti i messaggi in uscita delle liste di distribuzione. Poiché tutta la posta inviata alle liste di distribuzione viene firmata da MDaemon, per consentire la firma crittografica non è necessario utilizzare l'opzione "*Definire quali messaggi possono essere firmati*".

Per firmare la posta di una lista è necessario applicare il filtro contenuti a ciascun messaggio dopo la ripartizione della lista. Se le liste di distribuzione hanno grandi dimensioni e sono molto attive, ciò può determinare una diminuzione delle prestazioni del server.

Firma di default
Dall'elenco a discesa, scegliere il selettore di cui si desidera utilizzare la chiave pubblica/privata corrispondente quando si firmano i messaggi. Se si desidera creare una nuova coppia di chiavi con un selettore differente, digitare in questo campo il nome del selettore desiderato e selezionare l'opzione "*Creare nuove chiavi pubbliche e private*". Se si desidera firmare alcuni messaggi utilizzando un selettore alternativo, indicare un selettore specifico nell'opzione "*Definire quali messaggi possono essere firmati*" oppure creare una regola di Filtro contenuti utilizzando l'azione "*Firma con il selettore DKIM*" oppure "*Firma con il selettore DomainKeys*".

Elimina questo selettore
Per eliminare un selettore, fare clic su questo pulsante. Seguire le istruzioni visualizzate sullo schermo.

Creare nuove chiavi pubbliche e private
Fare clic su questo pulsante per generare una coppia di chiavi pubbliche o private per il selettore indicato precedentemente. Oltre alla coppia di chiavi viene generato il file `dns_readme.txt` che viene automaticamente aperto. Questo file contiene esempi di dati DK/DKIM che è necessario pubblicare nei record DNS del dominio, elencando i criteri di DK/DKIM e la chiave pubblica per il selettore specificato. Il file riporta esempi relativi sia allo stato di verifica che non, indicando se vengono firmati tutti i messaggi o solo alcuni fra quelli provenienti dal proprio dominio. Se si esegue una verifica DK/DKIM o del selettore, sarà necessario utilizzare le informazioni contenute nelle voci di Verifica relative ai criteri DomainKeys o al selettore, a seconda della verifica che si sta eseguendo. In caso contrario, sarà necessario utilizzare le voci di Non verificare.

Tutte le chiavi sono memorizzate in formato `PEM`. Tutti i selettori e le chiavi vengono salvati nella cartella `\MDaemon\Pem` con le modalità seguenti:

```
\MDaemon\Pem\<Selettore>\rsa.public - chiave pubblica per il
selettore
\MDaemon\Pem\<Selettore>\rsa.private - chiave privata per il
selettore.
```

I file contenuti in queste cartelle non sono né nascosti né crittografati. Tuttavia, è necessario impedire l'accesso non autorizzato a questi file, contenenti le chiavi crittografiche private RSA. È quindi necessario proteggere queste cartelle e le relative sottocartelle utilizzando gli strumenti disponibili nel sistema operativo in uso.

Definire quali messaggi possono essere firmati

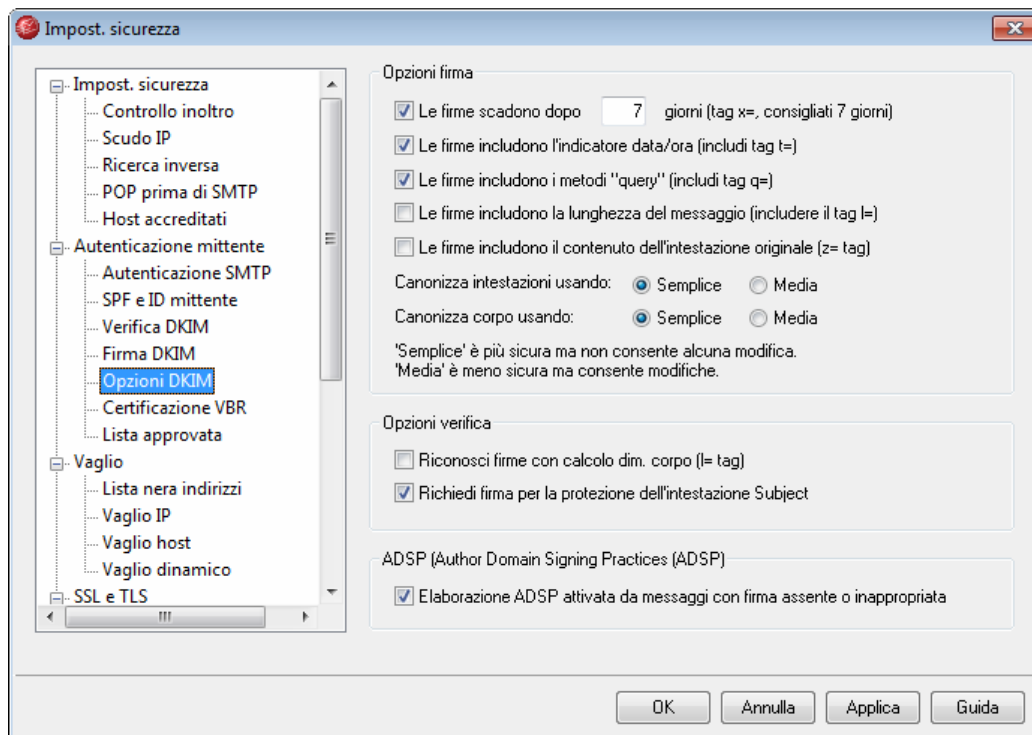
Una volta attivata una o entrambi le opzioni *Firma messaggi in uscita* descritte in precedenza, fare clic su questo pulsante per modificare il file `DKSign.dat` che contiene l'elenco dei domini e degli indirizzi utilizzati da MDaemon per stabilire se un messaggio debba essere firmato o meno. È necessario definire i messaggi da firmare in base agli indirizzi presenti in `To` o `From` oppure in base ad altre intestazioni del messaggio, ad esempio "`Reply-To`" o "`Sender`". È possibile, se si desidera, definire per ciascuna voce il selettore che verrà utilizzato quando si firma un messaggio corrispondente alla voce. Infine, è possibile specificare un dominio facoltativo per la firma da utilizzare nel tag "d=" dell'intestazione della firma. Questa caratteristica risulta utile, ad esempio, quando i messaggi vengono firmati da più sottodomini. In questi casi, è possibile utilizzare il tag "d=" per far sì che i server riceventi ricerchino le chiavi DomainKeys/DomainKeys Identified Mail nel record DNS di un solo dominio, in modo da gestire tutte le chiavi in un solo record anziché gestire i record separatamente per ciascun sottodominio. Nei domini e negli indirizzi sono accettati i caratteri jolly.

Possono essere firmati tutti i messaggi inviati da domini locali

Utilizzare questa opzione se si desidera che tutti i messaggi provenienti dai domini locali possano essere firmati. Se si utilizza questa opzione non è necessario aggiungere alcun altro dominio alla lista dei messaggi che è possibile firmare, ossia al file `DKSign.dat`, a meno che non si desideri indicare un selettore o un tag "`d=`" specifico da utilizzare per firmare i messaggi di un determinato dominio. L'opzione è abilitata per impostazione predefinita.

Per ulteriori informazioni, vedere:

DomainKeys Identified Mail (DKIM) 287
Opzioni DKIM 296
Verifica DKIM 289

5.4.2.3.3 Opzioni DKIM

Opzioni DKIM

Le firme scadono dopo XX giorni (tag x=, consigliati 7 giorni)
Se si desidera limitare la validità di una firma ad un numero di giorni, attivare questa opzione e indicare il numero di giorni desiderato. I messaggi con le firme scadute non superano mai la verifica. Questa opzione corrisponde al tag "x=" della firma. Per impostazione predefinita, questa opzione è abilitata con il valore preimpostato di 7 giorni.

Le firme includono l'indicatore data/ora (include tag t=)
Se si abilita questa opzione, nella firma viene incluso l'indicatore orario data-ora (tag "t=") di creazione della firma. Per impostazione predefinita, questa opzione è abilitata.

Le firme includono i metodi "query" (includi tag q=)
Per impostazione predefinita, questa funzione è abilitata. Con questa impostazione la firma include il tag relativo al metodo di interrogazione (ad esempio, "q=dns").

Le firme includono la lunghezza del messaggio (includi il tag l=)
Attivare questa opzione se si desidera includere nelle firme DKIM il tag relativo al calcolo della lunghezza del corpo del messaggio.

Le firme includono il contenuto dell'intestazione originale (tag z=)
Selezionare questa opzione se si desidera includere nelle firme DKIM il tag "z=". Il tag contiene una copia delle intestazioni originali dei messaggi. Questo potrebbe far aumentare notevolmente la dimensione della firma.

Canonizzazione

La canonizzazione è un processo tramite il quale le intestazioni e il corpo dei messaggi vengono convertiti in uno standard regolamentato e "normalizzati" prima della creazione di una firma DKIM. Questa operazione è necessaria poiché alcuni server di posta e sistemi di inoltro apportano durante l'elaborazione diverse modifiche al messaggio che possono causare malfunzionamenti se per la preparazione del messaggio non viene utilizzato uno standard "canonico". Al momento, sono disponibili due metodi di regolamentazione per la firma e la verifica DKIM: Semplice e Media. Il metodo semplice è quello più rigido e consente di apportare lievi modifiche al messaggio. Il metodo medio è meno rigido di quello semplice e consente di apportare al messaggio più modifiche, anche non consequenziali.

Canonizza intestazioni usando: Semplice, Media
Si tratta del metodo di canonizzazione utilizzato per le intestazioni dei messaggi al momento della firma. Il metodo Semplice non consente mai alcuna modifica ai campi di intestazione. Il metodo Media consente di convertire i nomi dell'intestazione (non i valori dell'intestazione) in lettere minuscole e uno o più spazi consecutivi in un unico spazio, nonché di apportare altre modifiche non di lieve entità. L'impostazione predefinita è "Semplice".

Canonizza corpo usando: Semplice, Media
Si tratta del metodo di canonizzazione utilizzato per il corpo del messaggio al momento della firma. Quello semplice ignora le righe vuote alla fine del corpo del messaggio e non consente alcuna altra modifica al corpo. Con il metodo Media, le righe vuote alla fine del messaggio sono consentite, gli spazi alla fine delle righe vengono ignorati, tutti gli spazi consecutivi di una riga vengono convertiti in un unico spazio ed è possibile apportare altre piccole modifiche. L'impostazione predefinita è "Semplice".

Opzioni verifica

Riconosci firme con calcolo dim. corpo ("l=" tag)
Quando viene attivata questa opzione, MDaemon riconoscerà il tag per il calcolo della dimensione del corpo trovato in una firma DKIM di un messaggio in entrata. Quando il calcolo della dimensione del corpo supera il valore contenuto nel tag, MDaemon eseguirà la verifica solo in base al valore indicato nel tag e il resto del messaggio non verrà verificato. Ciò indica che al messaggio sono stati aggiunti altri dati e che, di conseguenza, la porzione non verificata può essere considerata sospetta. Se il calcolo della lunghezza effettiva del messaggio è inferiore al valore contenuto nel tag, la firma non supera la verifica, ossia darà come risultato "`FAIL`". Ciò indica che una parte del messaggio è stata eliminata per cui il calcolo della lunghezza del messaggio risulta inferiore al valore indicato nel tag.

Richiedi firma per la protezione dell'intestazione Subject
Abilitare questa opzione se si desidera che la firma DKIM dei messaggi in entrata applichi la protezione all'intestazione Subject.

ADSP (Author Domain Signing Practices)

Elaborazione ADSP attivata da messaggi con firma assente o inappropriata
Abilitare questa opzione se si desidera ricercare e applicare record ADSP (Author

Domain Signing Practices) se un messaggio in entrata è privo di firma o se la firma non è appropriata. Se questa opzione è disabilitata o se il record ADSP utilizza una sintassi sconosciuta a MDaemon, il messaggio viene considerato come se il dominio firmasse solo alcuni messaggi.

Per ulteriori informazioni, vedere:

DomainKeys Identified Mail (DKIM) 287
Verifica DKIM 289
Firma DKIM 293

5.4.2.4 Certificazione dei messaggi

Nel processo di certificazione dei messaggi, un'entità garantisce o "certifica" la correttezza del comportamento relativo alla posta elettronica tenuto da un'altra entità. Di conseguenza, se l'entità certificante è accreditata presso un server di posta ricevente, i messaggi inviati da un dominio certificato da tale entità possono essere considerati più affidabili. Il server ricevente può ritenere, con un sufficiente grado di certezza, che il dominio mittente utilizza procedure ottimali relative alla posta e che non invia messaggi spam o altri messaggi contenenti rischi per la sicurezza. La certificazione rappresenta un vantaggio perché consente di evitare l'applicazione delle funzionalità di analisi antispam a messaggi per i quali non è necessaria, nonché di ridurre le risorse necessarie per l'elaborazione di ciascun messaggio.

MDaemon Pro supporta la certificazione dei messaggi grazie alla prima implementazione commerciale del nuovo protocollo di posta Internet VBR (Vouch-By-Reference). Alt-N Technologies si è impegnata e continua a impegnarsi per lo sviluppo di tale protocollo grazie alla partecipazione al DAC (Domain Assurance Council). Il protocollo VBR offre il meccanismo che consente ai CSP (Certification Service Provider, provider di servizi di certificazione) o alle entità "certificanti" di garantire la conformità a procedure ottimali relative alla posta elettronica utilizzate da specifici domini.

Certificazione dei messaggi in entrata

Per configurare la funzionalità di certificazione dei messaggi in entrata di MDaemon È sufficiente selezionare l'opzione *Abilita certificazione messaggi in entrata* della finestra di dialogo Certificazione VBR (Sicurezza » Impostazioni sicurezza » Autenticazione mittente » Certificazione VBR) e indicare uno o più provider di servizi di certificazione accreditati per la posta in entrata, ad esempio `vbr.emailcertification.org`. È inoltre possibile scegliere se escludere i messaggi certificati dall'elaborazione di Spam Filter o se correggerne il punteggio spam in senso positivo.

Certificazione dei messaggi in uscita

Per configurare l'inserimento dei dati di certificazione nei messaggi in uscita, è necessario disporre di uno o più CSP (Certification Service Provider) per la certificazione della posta. Alt-N Technologies offre ai propri clienti un servizio di certificazione. Per ulteriori informazioni, visitare: www.altn.com.

Per utilizzare la certificazione dei messaggi di posta in uscita con MDaemon, eseguire la

registrazione presso un provider CSP, quindi procedere come segue:

1. Aprire la finestra di dialogo Certificazione VBR, selezionando Sicurezza » Impostazioni sicurezza » Autenticazione mittente » Certificazione VBR.
2. Fare clic su "*Inserisci dati certificazione nei messaggi in uscita*."
3. Fare clic su "*Configura dominio per certificazione messaggi*". Verrà aperta la finestra di dialogo Impostazione certificazione.
4. Digitare il *Nome dominio* per il quale si desidera inserire i dati di certificazione nei messaggi in uscita.
5. Scegliere nell'elenco a discesa *Tipo di posta* il tipo di posta certificata dal CSP per il dominio oppure inserire un nuovo tipo di posta se quello desiderato non è presente.
6. Inserire uno o più CSP che certificheranno la posta in uscita del dominio. Separare i nomi dei CSP con uno spazio.
7. Fare clic su "*OK*".
8. Configurare il server in modo che esegua la firma dei messaggi in uscita del dominio utilizzando DKIM o DK 287 oppure utilizzare un server SPF o SIDF 285 approvato. Questa operazione è necessaria per garantire che l'origine del messaggio sia legittima, ossia che il messaggio proviene dal server MDaemon in uso. Un messaggio non può essere certificato se il server ricevente non è in grado di determinarne prima l'autenticità.

La tecnologia VBR non richiede che i messaggi siano firmati o che vengano trasmessi al CSP, perché quest'ultimo non si occupa della firma o della convalida di messaggi specifici, ma solo di garantire la conformità a procedure ottimali relative alla posta elettronica utilizzate da uno specifico dominio.

Per ulteriori informazioni sui servizi di certificazione forniti da Alt-N Technologies, visitare il sito:

http://www.altn.com/email-certification/

Per ulteriori informazioni su VBR e sulla certificazione dei messaggi, visitare il sito:

http://www.domain-assurance.org/

Bozza della specifica VBR – Internet-Draft 00:

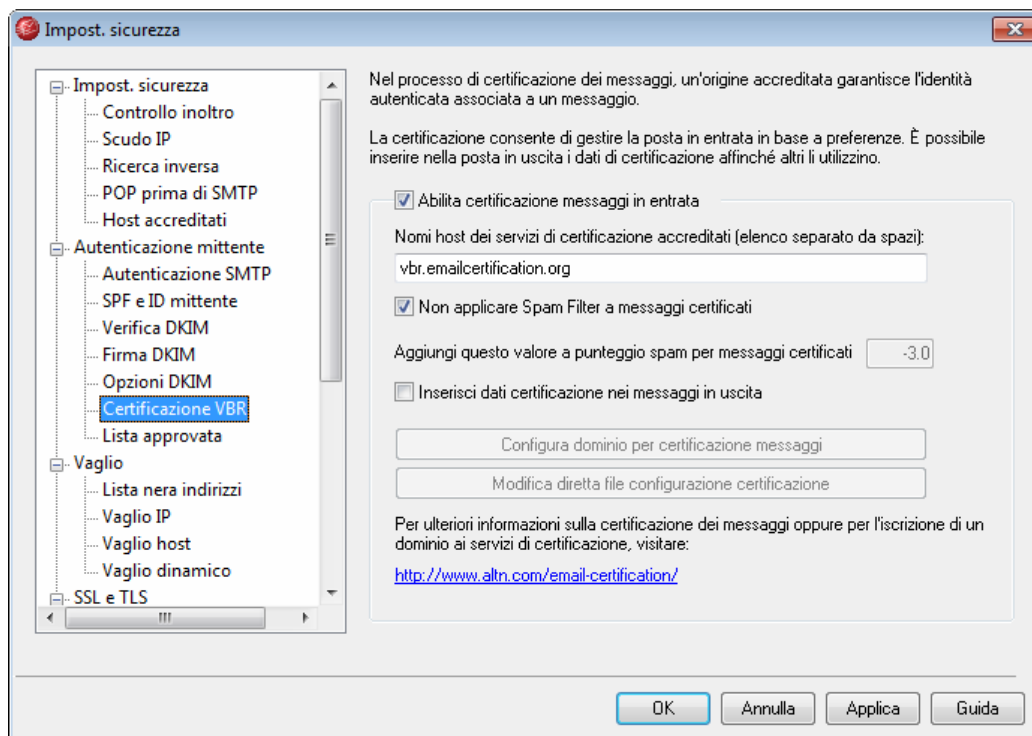
http://files.altn.com/MDaemon/drafts/draft-hoffman-dac-vbr-00.txt

Per ulteriori informazioni su DKIM, vedere:

http://www.dkim.org/

Per ulteriori informazioni, vedere:

Certificazione VBR 300

5.4.2.4.1 Certificazione VBR

La finestra di dialogo Certificazione VBR si trova in: Sicurezza » Impostazioni sicurezza » Autenticazione mittente » Certificazione VBR.

Certificazione dei messaggi

Abilita certificazione messaggi in entrata
Selezionare questa casella di controllo per abilitare la certificazione dei messaggi in entrata. Quando viene ricevuto un messaggio in entrata per il quale è richiesta la certificazione, MDaemon interroga il CSP (Certification Service Provider, provider di servizi di certificazione) accreditato per verificare se il messaggio possa essere considerato "certificato" o meno. In caso affermativo, a seconda dell'opzione selezionata il messaggio viene escluso dal filtro spam oppure viene corretto il punteggio assegnato da Spam Filter 243 al messaggio.

Nomi host dei servizi di certificazione accreditati (elenco separato da spazi):
Inserire in questa casella i nomi degli host accreditati per il servizio di certificazione. Nel caso di più host, separarne i nomi con uno spazio.

Non applicare Spam Filter a messaggi certificati
Scegliere questa opzione se si desidera escludere dal filtro spam i messaggi

certificati.

Aggiungi questo valore a punteggio spam per messaggi certificati
Se non si desidera escludere dal filtro spam i messaggi certificati, questa opzione consente di specificare il valore utilizzato per la rettifica del punteggio spam del messaggio. In genere, questo valore è un numero negativo che rappresenta una rettifica in senso positivo del punteggio spam. Il valore predefinito è "`-3.0`".

Inserisci dati certificazione nei messaggi in uscita
Fare clic su questa casella di controllo per inserire i dati di certificazione nei messaggi in uscita. Fare quindi clic sul pulsante *Configura dominio per certificazione messaggi* per aprire la finestra di dialogo Impostazione certificazione al fine di specificare i domini da certificare e i relativi CSP.

Configura dominio per certificazione messaggi
Dopo aver selezionato l'opzione *Inserisci dati certificazione nei messaggi in uscita*, fare clic su questo pulsante per aprire la finestra di dialogo Impostazione certificazione. Nella finestra di dialogo è possibile specificare il dominio associato ai messaggi in uscita da certificare, i tipi di posta da certificare e i CSP associati al dominio.

Modifica diretta file configurazione certificazione
Dopo aver selezionato l'opzione *Inserisci dati certificazione nei messaggi in uscita*, fare clic su questo pulsante per aprire il file di configurazione VBR (Vouch-by-Reference). Il file include tutti i domini configurati nella finestra di dialogo Impostazione certificazione per l'uso di VBR, unitamente ai relativi dati VBR. È possibile utilizzare questo file per modificare le voci precedentemente create o per crearne di nuove.

Impostazione certificazione

Dopo aver abilitato l'opzione *Inserisci dati certificazione nei messaggi in uscita* della finestra di dialogo Certificazione, fare clic sul pulsante *Configura dominio per certificazione messaggi* per aprire la finestra di dialogo Impostazione certificazione. Nella finestra di dialogo è possibile specificare il dominio associato ai messaggi in uscita da certificare, i tipi di posta da certificare e i CSP associati al dominio.

Impostazione certificazione

Nome dominio
Utilizzare questa opzione per inserire il dominio per il quale certificare i messaggi in uscita.

Trova
Se la funzione di certificazione dei messaggi è stata già configurata per uno specifico dominio, digitare il *Nome dominio* e fare clic su questo pulsante per inserire nella finestra di dialogo le opzioni già definite.

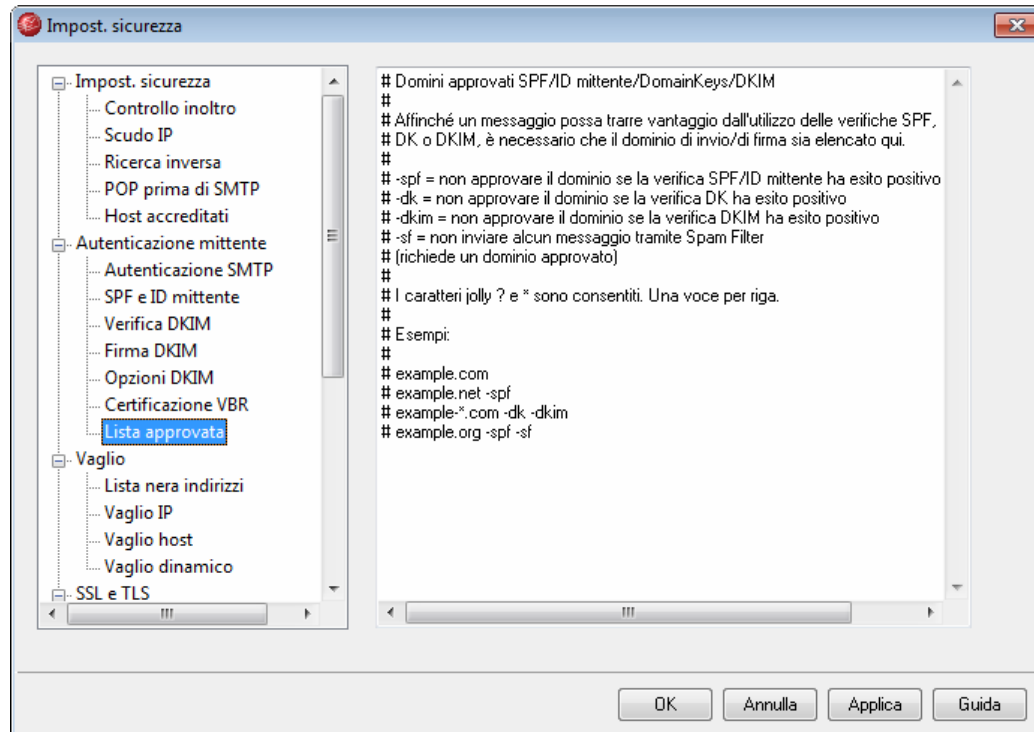
Tipo di posta
Utilizzare la casella di riepilogo a discesa per scegliere il tipo di posta certificata in relazione al dominio dal CSP associato. Se il tipo desiderato non è presente, inserirne uno manualmente.

Nomi host dei servizi...
Inserire i nomi degli host dei CSP accreditati per la certificazione dei messaggi in

uscita del dominio, ad esempio `vbr.emailcertification.org`. Nel caso di più CSP, separarne i nomi con uno spazio.

Per ulteriori informazioni, vedere

Certificazione dei messaggi 298

5.4.2.5 Lista approvata

Poiché alcuni spammer e autori di posta collettiva hanno iniziato ad utilizzare SPF o a firmare i messaggi con firme DK o DKIM valide, il fatto che un messaggio sia stato firmato e verificato non garantisce che non debba essere considerato uno spam, né assicura che il messaggio provenga da un'origine sicura. Per questo motivo, il punteggio di spam di un messaggio non viene ridotto in conseguenza di una verifica SPF, ID mittente, DK o DKIM, a meno che il dominio individuato mediante la firma non si trovi nell'elenco approvato che consiste, sostanzialmente, in una lista bianca che indica i domini per i quali è consentita la riduzione dei punteggi di spam dei messaggi in arrivo dopo la loro verifica.

Quando un messaggio firmato da uno di questi domini viene verificato da SPF, ID mittente, DK o DKIM, il relativo punteggio di spam viene ridotto in base alle impostazioni che si trovano nelle schermate SPF e ID mittente 285 e Verifica DKIM 289. È comunque possibile allegare una qualsiasi combinazione dei flag elencati di seguito, se si desidera impedire ad uno o più di tali metodi di verifica di ridurre il punteggio. È inoltre disponibile un flag che consente di impedire ai messaggi verificati il passaggio attraverso Spam Filter.

-spf Non ridurre il punteggio di spam nel caso di messaggi verificati da SPF o ID

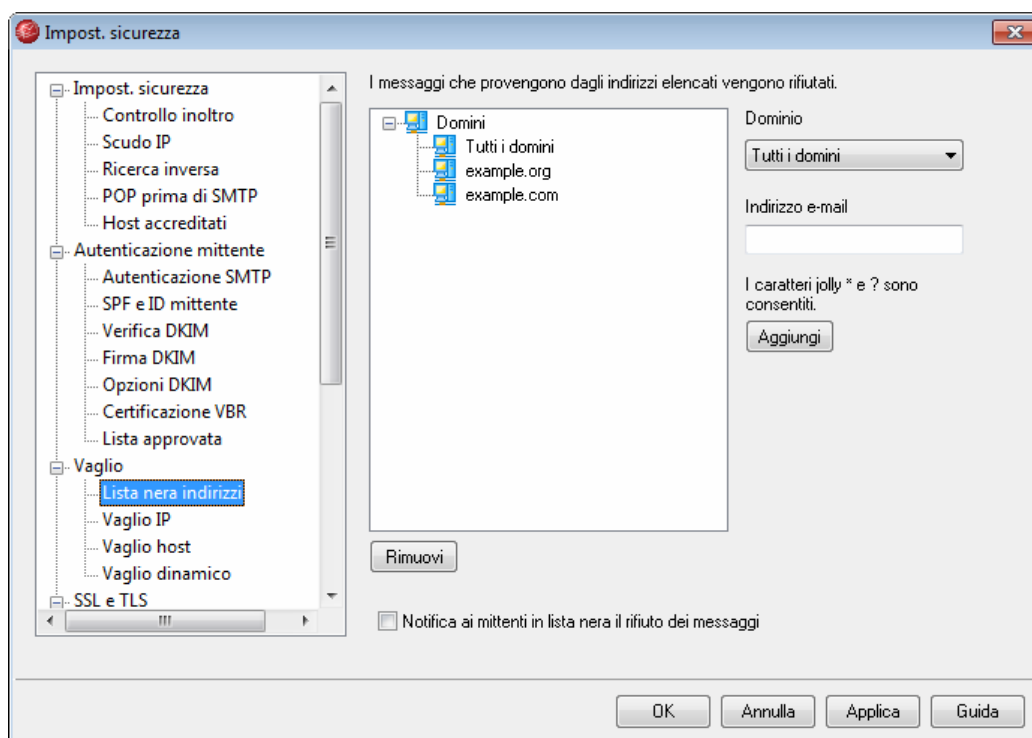
mittente inviati da questo dominio.

-dk Non ridurre il punteggio di spam nel caso di messaggi verificati da DK inviati da questo dominio.

-dkim Non ridurre il punteggio di spam nel caso di messaggi verificati da DKIM inviati da questo dominio.

-sf Non elaborare i messaggi verificati da questo dominio tramite Spam Filter.

5.4.3 Vaglio

5.4.3.1 Lista nera indirizzi

La funzionalità Lista nera indirizzi è disponibile in: Sicurezza» Impostazioni sicurezza» Vaglio. Questo elenco contiene gli indirizzi che non sono autorizzati a inviare posta mediante il server. I messaggi provenienti da uno degli indirizzi della lista nera vengono respinti durante la sessione SMTP. Questo metodo è utile per limitare alcuni dei problemi degli utenti. Gli indirizzi possono essere inseriti nella lista nera a livello di singolo dominio o in modo globale, ossia in tutti i domini di MDaemon.

I messaggi che provengono dagli indirizzi elencati vengono rifiutati
Questa finestra visualizza tutti gli indirizzi attualmente inseriti in lista nera, suddivisi per dominio.

Dominio
Scegliere il dominio al quale verrà associato l'indirizzo inserito nella lista nera, ossia il dominio che non deve più ricevere posta proveniente dall'indirizzo specificato. Per

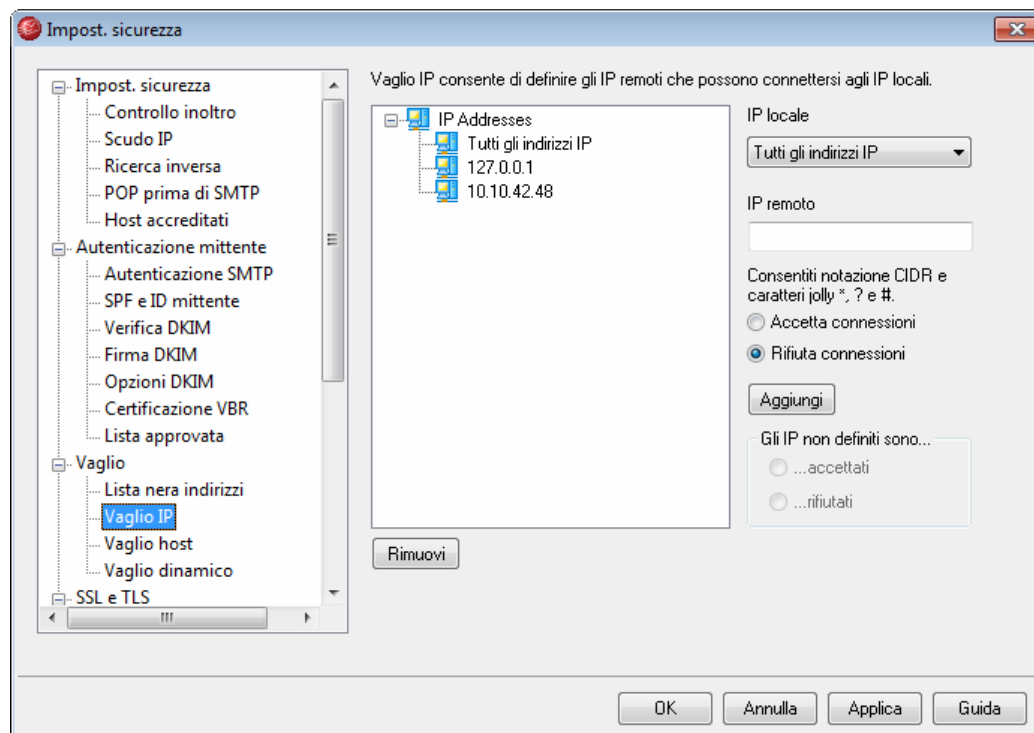
inserire in lista nera l'indirizzo a livello di tutti i domini, scegliere "All Domains" (Tutti i domini).

Indirizzo e-mail
Immettere l'indirizzo da inserire in lista nera. Poiché sono consentiti i caratteri jolly, la sintassi "*@badmail.com" sopprime tutti i messaggi provenienti da tutti gli utenti di "badmail.com" e la sintassi "franco@*" sopprime tutti i messaggi da tutti gli indirizzi che iniziano con "franco", indipendentemente dal dominio di partenza del messaggio.

Aggiungi
Fare clic su questo pulsante per aggiungere alla lista nera l'indirizzo specificato.

Rimuovi
Fare clic su questo pulsante per rimuovere dall'elenco la voce selezionata.

Notifica ai mittenti in lista nera il rifiuto dei messaggi
Se questa opzione è abilitata, all'indirizzo inserito nella lista nera viene inviato un messaggio al fine di segnalare che il messaggio è stato eliminato.

5.4.3.2 Vaglio IP

Vaglio IP è disponibile in: Sicurezza » Impostazioni sicurezza» Vaglio. Vaglio IP consente di definire gli indirizzi IP remoti autorizzati a connettersi con gli indirizzi IP locali. L'accettazione o il rifiuto delle richieste di connessione può essere associato

all'intero elenco degli indirizzi IP oppure a uno o più indirizzi. Gli indirizzi IP remoti inseriti in Vaglio IP possono essere associati con tutti gli indirizzi IP locali o con singoli indirizzi IP. È consentito l'uso della notazione CIDR e dei caratteri jolly *, # e ?.

Ad esempio:

..*.*	Corrisponde a tutti gli indirizzi IP
#.#.#.#	Corrisponde a tutti gli indirizzi IP
192.*.*.*	Corrisponde a tutti gli indirizzi IP che iniziano con 192
192.168.*.239	Corrisponde agli indirizzi IP da 192.168.0.239 a 192.168.255.239
192.168.0.1??	Corrisponde agli indirizzi IP da 192.168.0.100 a 192.168.0.199

IP locale
Nell'elenco a discesa, scegliere "All IP" o l'indirizzo IP locale al quale applicare le impostazioni della schermata.

IP remoto
Inserire l'indirizzo IP remoto da aggiungere all'elenco, associato con l'IP locale indicato in precedenza.

Accetta connessioni
Selezionando questa opzione, si autorizza la connessione degli indirizzi IP remoti specificati con l'indirizzo IP locale associato.

Rifiuta connessioni
Selezionando questa opzione, NON si autorizza la connessione degli indirizzi IP remoti specificati con l'indirizzo IP locale associato. La connessione verrà rifiutata o eliminata.

Aggiungi
Dopo aver inserito le informazioni relative alle opzioni precedenti, fare clic su questo pulsante per aggiungere la voce all'elenco.

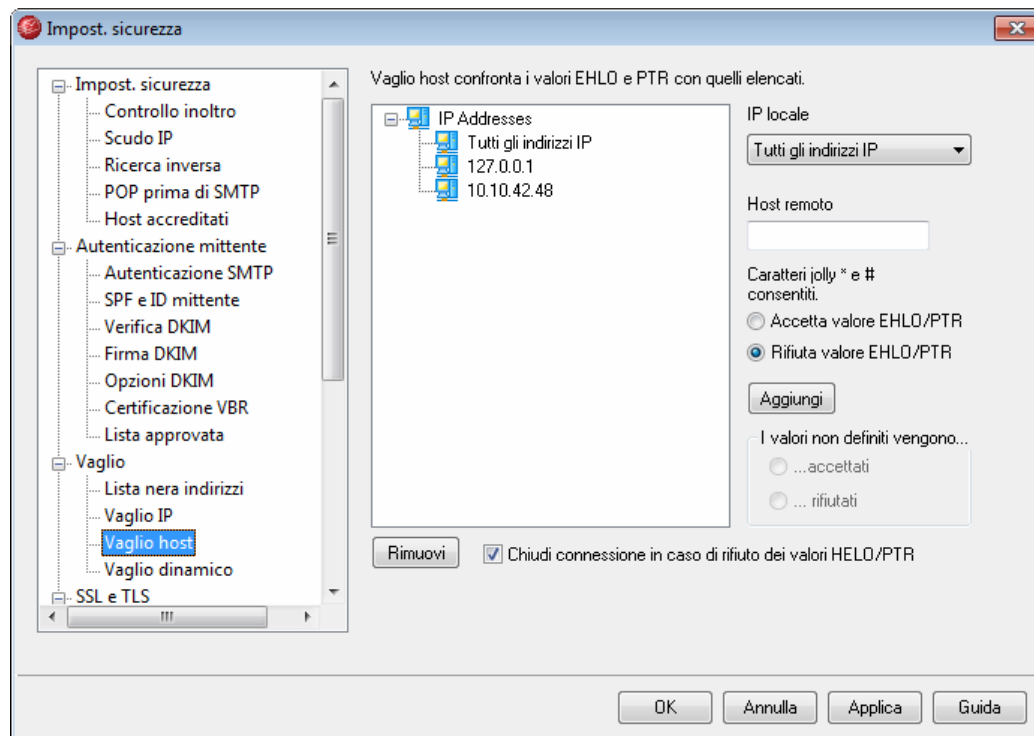
Rimuovi
Per rimuovere una voce dall'elenco, selezionarla e fare clic su questo pulsante.

Gli IP non definiti sono...

...accettati
Scegliendo questa opzione, verranno accettate le connessioni provenienti da qualsiasi indirizzo IP non espressamente definito nella schermata Vaglio IP.

...rifiutati
Scegliendo questa opzione, verranno respinte o eliminate le connessioni provenienti da qualsiasi indirizzo IP non espressamente definito nella schermata Vaglio IP.

Vaglio IP non bloccherà in nessun caso gli indirizzi IP accreditati 282 o locali .

5.4.3.3 Vaglio host

Vaglio host è disponibile in: Sicurezza » Impostazioni sicurezza» Vaglio. Vaglio host consente di definire gli host remoti autorizzati a connettersi agli indirizzi IP locali. È possibile specificare un elenco di host e configurare il server in modo che autorizzi o rifiuti le connessioni dagli host indicati. Vaglio host esegue un confronto tra i valori EHLO e PTR, determinati nel corso della sessione SMTP, e i valori indicati in questa schermata.

IP locale
Con questo elenco a discesa è possibile scegliere l'indirizzo IP locale al quale applicare questa voce di Vaglio host. Per applicarla a tutti gli indirizzi IP locali, selezionare "All IPs".

Host remoto
Inserire l'host remoto da aggiungere all'elenco, associato con l'IP locale indicato in precedenza.

Accetta valore EHLO/PTR
Selezionando questa opzione, si autorizza la connessione dell'host remoto specificato con l'indirizzo IP locale associato.

Rifiuta valore EHLO/PTR
Selezionando questa opzione, NON si autorizza la connessione dell'host remoto specificato con l'indirizzo IP locale associato. La connessione viene rifiutata oppure

eliminata se si è abilitata l'opzione "*Chiudi connessione in caso di rifiuto dei valori HELO/PTR*".

Aggiungi
Dopo aver inserito le informazioni relative alle opzioni precedenti, fare clic su questo pulsante per aggiungere la voce all'elenco.

Rimuovi
Per rimuovere una voce dall'elenco, selezionarla e fare clic su questo pulsante.

Gli host non definiti sono...

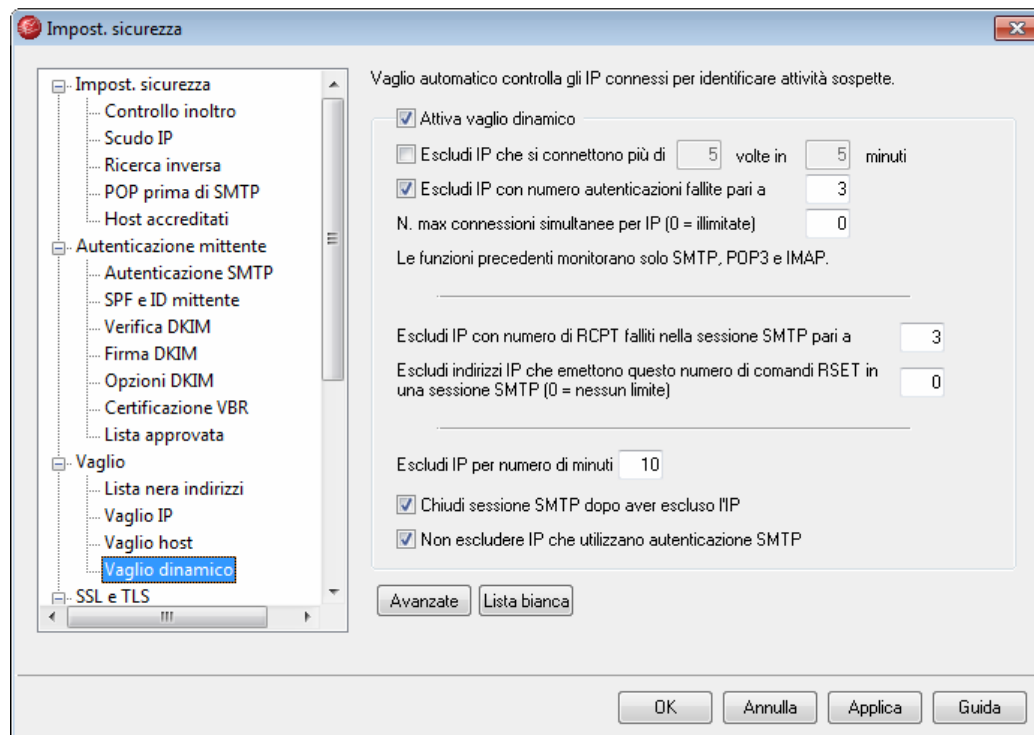
...accettati
Scegliendo questa opzione, verranno accettate le connessioni provenienti da qualsiasi host non espressamente definito nella schermata Vaglio host.

...rifiutati
Scegliendo questa opzione, verranno rifiutate le connessioni provenienti da qualsiasi host non espressamente definito nella schermata Vaglio host.

La schermata relativa a Vaglio host non bloccherà in nessun caso gli host accreditati 282 o quelli locali.

Chiudi connessione in caso di rifiuto dei valori HELO/PTR

Questa casella di controllo consente di chiudere la connessione quando la configurazione impostata nella schermata Vaglio host prevede il rifiuto del valore HELO/PTR.

5.4.3.4 Vaglio dinamico

Utilizzando le funzioni di vaglio dinamico, MDaemon è in grado di tenere traccia del comportamento dei server di invio per identificare attività sospette e rispondere di conseguenza. Ad esempio, è possibile escludere momentaneamente un indirizzo IP da future connessioni al server, a seguito di un determinato numero di errori relativi a "destinatario sconosciuto" verificatisi durante la connessione di posta dall'indirizzo stesso. È inoltre possibile escludere i mittenti che si connettono al server più di un determinato numero di volte per più minuti e i mittenti che falliscono i tentativi di connessione più volte.

L'esclusione del mittente non è permanente, ma viene applicata solo per il numero di minuti indicati all'interno della finestra di dialogo. Inoltre, con il pulsante *Avanzate* di questa finestra di dialogo è possibile aprire il file `DynamicScreen.dat` che contiene l'elenco degli indirizzi IP esclusi e la durata dell'esclusione relativa a ciascun indirizzo. Questo file risiede nella memoria e può essere modificato premendo il pulsante *Avanzate* oppure con un editor di testo. Nota: modificando manualmente questo file, è possibile creare un file vuoto, denominato `TARPIT.SEM`, e collocarlo nella directory `\APP\` di MDaemon. In questo modo, MDaemon carica nuovamente il file `DynamicScreen.dat` residente in memoria implementando così le modifiche.

Vaglio dinamico

Attiva vaglio dinamico
Per attivare la funzione di vaglio automatico, selezionare questa casella di controllo.

Escludi mittenti che si connettono più di [X] volte in [X] minuti
Selezionare questa casella di controllo se si desidera escludere momentaneamente i siti che si connettono un numero eccessivo di volte al proprio server in un intervallo

di tempo limitato. Specificare il numero di minuti e di connessioni consentiti durante questo intervallo.

Escludi IP con numero autenticazioni fallite pari a
Indicare in questo campo il numero di tentativi di autenticazione falliti superato il quale si desidera escludere momentaneamente i siti. In questo modo è possibile impedire gli attacchi degli hacker e le sessioni autenticate illegalmente. Questa opzione controlla le connessioni SMTP, POP3 e IMAP.

N. max connessioni simultanee per IP (0 = illimitate)
Indica il numero massimo di connessioni simultanee consentite da un singolo indirizzo IP prima che venga escluso. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

Escludi IP con numero di RCPT falliti nella sessione SMTP pari a
Quando un indirizzo IP provoca un determinato numero di errori di tipo "Destinatario sconosciuto" durante una sessione di posta, verrà automaticamente escluso per il numero di minuti specificato nel campo *Escludi IP per numero di minuti*. Frequenti errori di tipo "Destinatario sconosciuto" rappresentano spesso un indizio del fatto che il mittente sia uno "spammer" in quanto, generalmente, in questo caso i messaggi vengono inviati a indirizzi obsoleti o errati.

Escludi indirizzi IP che emettono questo numero di comandi RSET in una sessione SMTP (0 = nessun limite)
Questa opzione consente di escludere un indirizzo IP che abbia prodotto il numero di comandi RSET indicato. Inserire "0" se non si desidera impostare alcun limite. Nella schermata Server46 di Dominio predefinito/server esiste un'opzione simile che consente di limitare il numero di comandi RSET consentito.

Escludi IP per numero di minuti
Quando un indirizzo IP viene escluso automaticamente, in questa casella viene indicata la durata dell'esclusione espressa in minuti. Allo scadere dell'esclusione, i messaggi inviati dall'indirizzo IP verranno ricevuti normalmente. La funzione, dunque, impedisce di escludere accidentalmente un indirizzo IP valido in modo definitivo.

Chiudi sessione SMTP dopo aver escluso l'IP
Attivando questa opzione, MDaemon chiude la sessione SMTP dopo l'esclusione dell'indirizzo IP.

Non escludere IP che utilizzano autenticazione SMTP
Selezionando questa casella di controllo, i mittenti che autenticano le sessioni di posta prima dell'invio non vengono interessati dal vaglio dinamico.

Avanzate
Per aprire l'elenco esclusioni archiviato nel file `DynamicScreen.dat`, fare clic su questo pulsante. Nel file vengono elencati tutti gli indirizzi IP esclusi dal vaglio automatico. Per aggiungere manualmente gli indirizzi IP e il numero di minuti di esclusione, inserirli in un elenco, una voce per ciascuna riga, come descritto di seguito: `Indirizzo_IP<spazio>Minuti`. Ad esempio, `1.2.3.4 60`.

Lista bianca
Fare clic su questo pulsante per aprire la finestra di dialogo relativa alla lista bianca delle esclusioni dal vaglio dinamico. Gli indirizzi IP inclusi nell'elenco vengono esclusi dalle funzioni di tarpitting e di vaglio dinamico.

5.4.4 SSL e TLS

MDaemon include il supporto dei protocolli SSL (Secure Sockets Layer) e TLS (Transport Layer Security) per SMTP, POP, IMAP e per il server Web di WorldClient. Il protocollo SSL, sviluppato da Netscape Communications Corporation, è il metodo standard per la protezione delle comunicazioni Web tra server e client e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché SSL è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL quando ci si connette a WorldClient.

Se si effettua una connessione a porte di posta standard tramite un client di posta anziché tramite WorldClient, MDaemon supporta l'estensione STARTTLS su TLS per SMTP e IMAP, nonché l'estensione STLS per POP3. Tuttavia, è necessario che il client sia configurato per l'uso di SSL e che supporti queste estensioni, dal momento che non tutti i client prevedono tale supporto.

Infine, è possibile dedicare specifiche porte per le connessioni SSL. Ciò non è obbligatorio ma consente di fornire un livello di accessibilità più elevato ai client che non supportano alcune estensioni SSL. Ad esempio, alcune versioni di Microsoft Outlook Express non supportano l'estensione STARTTLS per IMAP sulla porta di posta predefinita, mentre supportano le connessioni a porte SSL dedicate.

Le opzioni che consentono di abilitare e configurare il protocollo SSL si trovano nella sezione SSL e TLS della finestra di dialogo Impostazioni sicurezza, disponibile in Sicurezza» Impostazioni sicurezza» SSL e TLS. Le impostazioni delle porte SSL per i protocolli SMTP, POP3 e IMAP si trovano nella finestra Porte 49, accessibile dal percorso: Impostazioni » Dominio predefinito/server.

Per ulteriori informazioni sulla creazione e l'uso dei certificati SSL, vedere:

Creazione e uso dei certificati SSL 320

-

Il protocollo TLS/SSL viene descritto nella RFC-2246, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2246.txt.

L'estensione STARTTLS per SMTP viene descritta nella RFC-3207, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc3207.txt.

L'uso di TLS con i protocolli IMAP e POP3 viene descritto nella RFC-2595, consultabile su Internet all'indirizzo

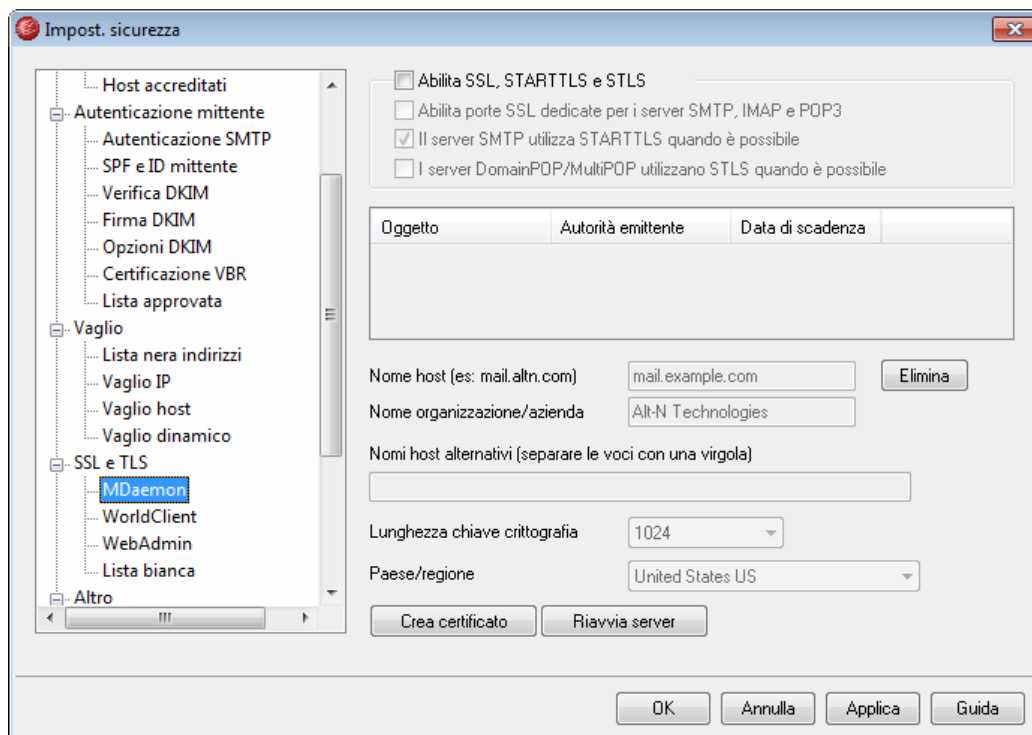
http://www.rfc-editor.org/rfc/rfc2595.txt.

Per ulteriori informazioni, vedere:

SSL e TLS » MDaemon 312

SSL e TLS » WorldClient 314

SSL e TLS » WebAdmin 317

5.4.4.1 MDaemon

Abilita SSL, STARTTLS e STLS
Selezionare questa casella di controllo per attivare il supporto per i protocolli SSL/TLS e le estensioni STARTTLS e STLS, quindi scegliere il certificato che si desidera utilizzare nell'elenco successivo.

Abilita porte SSL dedicate per i server SMTP, IMAP e POP3
Selezionare questa opzione per abilitare le porte SSL dedicate, specificate nella finestra Porte 49 di Dominio predefinito/server. Ciò non condiziona l'uso da parte dei client di STARTTLS e STLS con le porte di posta predefinite, ma fornisce solo un livello di supporto maggiore per il protocollo SSL.

Il server SMTP utilizza STARTTLS quando è possibile
Selezionare questa opzione per tentare di utilizzare l'estensione STARTTLS per tutti i messaggi SMTP inviati. Se il server al quale ci si connette non supporta l'estensione STARTTLS, il messaggio viene consegnato normalmente senza utilizzare il protocollo SSL. Utilizzare la Lista bianca320 di questa sezione per impedire l'utilizzo di STARTTLS per alcuni domini.

I server DomainPOP/MultiPOP utilizzano STLS quando è possibile
Selezionare questa casella di controllo per fare in modo che i server DomainPOP e MultiPOP utilizzino l'estensione STLS ogniqualvolta sia possibile.

Elenco certificati

Questa casella consente di visualizzare i certificati SSL. Per definire quale certificato debbano utilizzare i server di posta, selezionarlo dall'elenco. Fare doppio clic sul certificato per aprire la finestra di dialogo Certificato che consente di visualizzarne i dettagli.

MDaemon non offre il supporto di certificati diversi per più domini. Tutti i domini di posta devono condividere un unico certificato. Se si dispone di più domini inserirne i nomi nel campo *Nomi host alternativi (separare le voci con una virgola)* descritto di seguito.

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Viene visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Per creare i certificati si utilizzano i seguenti controlli. Per modificare il certificato, selezionarlo dall'elenco precedente.

Nome host
Inserire il nome host da utilizzare per la connessione (ad esempio, "posta.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Il supporto di più certificati per più domini non è disponibile in MDaemon. Tutti i domini devono condividere un unico certificato. Qualora esistano nomi host alternativi per le connessioni degli utenti e nel caso in cui si intenda applicare il certificato anche a tali nomi, inserire i nomi dei domini separati da virgole. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Crea certificato
Dopo aver inserito tutte le informazioni nei controlli descritti in precedenza, per creare il certificato fare clic su questo pulsante.

Riavvia server
Per riavviare i server SMTP/IMAP/POP, fare clic su questa opzione. Quando vengono apportate delle modifiche al certificato, è necessario riavviare i server.

Vedere:

SSL e TLS 311
Creazione e uso dei certificati SSL 320

5.4.4.2 WorldClient

Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). Il protocollo SSL, sviluppato da Netscape Communications

Corporation, è il metodo standard per la protezione delle comunicazioni Web server/client e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare WebAdmin per l'utilizzo di HTTPS si trovano nella schermata SSL/HTTPS, disponibile in Impostazioni » Web, Sincronizzazione e Servizi IM » WebAdmin (configurazione Web)". Per praticità, tali impostazioni sono presenti anche in "Sicurezza» Impostazioni sicurezza » SSL e TLS » WorldClient".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: SSL e TLS 311.

Questa schermata è valida per WorldClient solo quando si utilizza il server Web incorporato di MDaemon. Se si configura WebAdmin per l'esecuzione con altri server Web quali IIS, queste opzioni non sono disponibili. Il supporto per SSL/HTTPS dovrà essere configurato con gli strumenti offerti dal server Web utilizzato.

Tipi di connessioni accettate

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a WorldClient. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in WorldClient, ma non si desidera imporre agli utenti di WorldClient l'utilizzo di HTTPS. WorldClient rimane in attesa di connessioni sulla porta HTTPS indicata di seguito, ma risponde anche alle normali connessioni HTTP sulla porta di WorldClient definita nella scheda Server Web 123 della schermata WorldClient (posta Web).

Solo HTTPS
Scegliere questa opzione se si desidera richiedere l'utilizzo di HTTPS al momento della connessione a WorldClient. Se si attiva questa opzione, WorldClient risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da WorldClient per le connessioni SSL. La porta SSL predefinita è 443. Se si utilizza la porta predefinita, per le connessioni HTTPS non è necessario includere il numero della porta nell'URL di WorldClient (vale a dire, "https://esempio.com" è equivalente a "https://esempio.com:443").

Questa porta è diversa dalla porta di WorldClient definita nella scheda Server Web[123] della schermata WorldClient (posta Web). Se le connessioni HTTP a WorldClient sono consentite, devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

Certificati

Questa casella consente di visualizzare i certificati SSL. Per definire il certificato da utilizzare in WorldClient, selezionarlo dall'elenco. Fare doppio clic sul certificato per aprire la finestra di dialogo Certificato che consente di visualizzarne o modificarne i dettagli.

MDaemon non consente l'utilizzo di più certificati per WorldClient. Tutti i domini WorldClient devono condividere un unico certificato. Qualora sia disponibile più di un dominio, inserire i nomi di tali domini e di quelli che si intende utilizzare per accedere a WebAdmin nel campo denominato "*Nomi host alternativi (separare le voci con una virgola)*" descritto di seguito.

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wc.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Il supporto di più certificati non è disponibile. Tutti i domini WorldClient devono condividere un unico certificato. Qualora per le connessioni degli utenti esistano nomi host alternativi, inserire i nomi dei domini separati da virgole nel caso in cui si intenda applicare il certificato anche ai nomi alternativi. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Crea certificato
Dopo aver inserito tutte le informazioni nei controlli descritti in precedenza, per creare il certificato fare clic su questo pulsante.

Riavvia server Web
Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare i nuovi certificati, è necessario riavviare il server Web.

Per ulteriori informazioni, vedere:

SSL e TLS 311
Creazione e uso dei certificati SSL 320

5.4.4.3 WebAdmin

Nel server Web incorporato di MDaemon è stato aggiunto il supporto del protocollo SSL (Secure Sockets Layer). Il protocollo SSL, sviluppato da Netscape Communications Corporation, è il metodo standard per la protezione delle comunicazioni Web server/client e offre funzioni per l'autenticazione server, la crittografia dei dati e l'autenticazione dei client per le connessioni TCP/IP. Inoltre, poiché il supporto al protocollo HTTPS (ossia HTTP su SSL) è incorporato in tutti i browser più diffusi, è sufficiente installare un certificato digitale nel server per attivare le funzionalità SSL dei client connessi.

Le opzioni che consentono di abilitare e configurare WebAdmin per l'utilizzo di HTTPS si trovano nella schermata SSL/HTTPS, disponibile in Impostazioni » Web,

Sincronizzazione e Servizi IM » WebAdmin (configurazione Web)". Per praticità, tali impostazioni sono presenti anche in "Sicurezza» Impostazioni sicurezza » SSL e TLS » WebAdmin".

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere: **SSL e TLS** 311.

Questa schermata è valida per WebAdmin solo quando si utilizza il server Web incorporato di MDaemon. Se si configura WebAdmin per l'esecuzione con altri server Web quali IIS, queste opzioni non sono disponibili. Il supporto per SSL/HTTPS dovrà essere configurato con gli strumenti offerti dal server Web utilizzato.

Tipi di connessioni accettate

Solo HTTP
Scegliere questa opzione se non si desidera consentire alcuna connessione HTTPS a WebAdmin. Saranno consentite solo le connessioni HTTP.

HTTP e HTTPS
Scegliere questa opzione se si desidera attivare il supporto SSL in WebAdmin, ma non si desidera imporre agli utenti di WebAdmin l'utilizzo di HTTPS. WebAdmin rimane in attesa di connessioni sulla *porta HTTPS* indicata di seguito, ma risponde anche alle normali connessioni HTTP sulla porta TCP di WebAdmin definita nella schermata Server Web 145 di WebAdmin (configurazione Web).

Solo HTTPS
Scegliere questa opzione se si desidera richiedere l'utilizzo di HTTPS al momento della connessione a WebAdmin. Se si attiva questa opzione, WebAdmin risponde solo a connessioni HTTPS e ignora le richieste HTTP.

HTTP reindirizzato su HTTPS
Scegliere questa opzione se si desidera reindirizzare le connessioni HTTP al protocollo HTTPS sulla porta HTTPS.

Porta HTTPS
Consente di specificare la porta TCP utilizzata da WebAdmin per le connessioni SSL. La porta SSL predefinita è 443. Se si utilizza la porta predefinita, per le connessioni HTTPS non è necessario includere il numero della porta nell'URL di WebAdmin (vale a dire, "https://esempio.com" è equivalente a "https://esempio.com:443").

Questa porta è diversa dalla porta di WebAdmin definita nella scheda Server Web 145 della schermata WebAdmin (configurazione Web). Se consentite, le connessioni HTTP a WebAdmin devono utilizzare quest'ultima porta. Le connessioni HTTPS devono utilizzare la porta HTTPS.

Certificati

Questa casella consente di visualizzare i certificati SSL. Per definire il certificato da utilizzare in WebAdmin, selezionarlo dall'elenco. Fare doppio clic sul certificato per aprire la finestra di dialogo Certificato che consente di visualizzarne o modificarne i dettagli.

MDaemon non consente l'utilizzo di più certificati per WebAdmin. Tutti i domini devono condividere un unico certificato. Qualora sia disponibile più di un dominio, inserire i nomi di tali domini e di quelli che si intende utilizzare per accedere a WebAdmin nel campo denominato "*Nomi host alternativi (separare le voci con una virgola)*" descritto di seguito.

Elimina
Per eliminare un certificato, selezionarlo dall'elenco e fare clic su questo pulsante. Verrà visualizzata una finestra che richiede di confermare l'eliminazione del certificato.

Nome host
In fase di creazione di un certificato, inserire il nome host da utilizzare per la connessione (ad esempio, "wa.esempio.com").

Nome organizzazione/azienda
Inserire il nome dell'organizzazione o dell'azienda "proprietaria" del certificato.

Nomi host alternativi (separare le voci con una virgola)
Il supporto di più certificati non è disponibile. Tutti i domini devono condividere un unico certificato. Qualora per le connessioni degli utenti esistano nomi host alternativi, inserire i nomi dei domini separati da virgole nel caso in cui si intenda applicare il certificato anche ai nomi alternativi. Sono ammessi i caratteri jolly, ad esempio "`*.esempio.com`" indica tutti i sottodomini di `esempio.com` ("`wc.esempio.com`", "`posta.esempio.com`" e così via).

Lunghezza chiave crittografia
Scegliere la lunghezza della chiave crittografica relativa al certificato. Maggiore è la lunghezza della chiave, maggiore è la protezione dei dati trasferiti. Si noti che non tutte le applicazioni offrono il supporto per chiavi con lunghezza maggiore di 512.

Paese/regione
Scegliere il Paese o la regione in cui si trova il server.

Crea certificato
Dopo aver inserito tutte le informazioni nei controlli descritti in precedenza, per creare il certificato fare clic su questo pulsante.

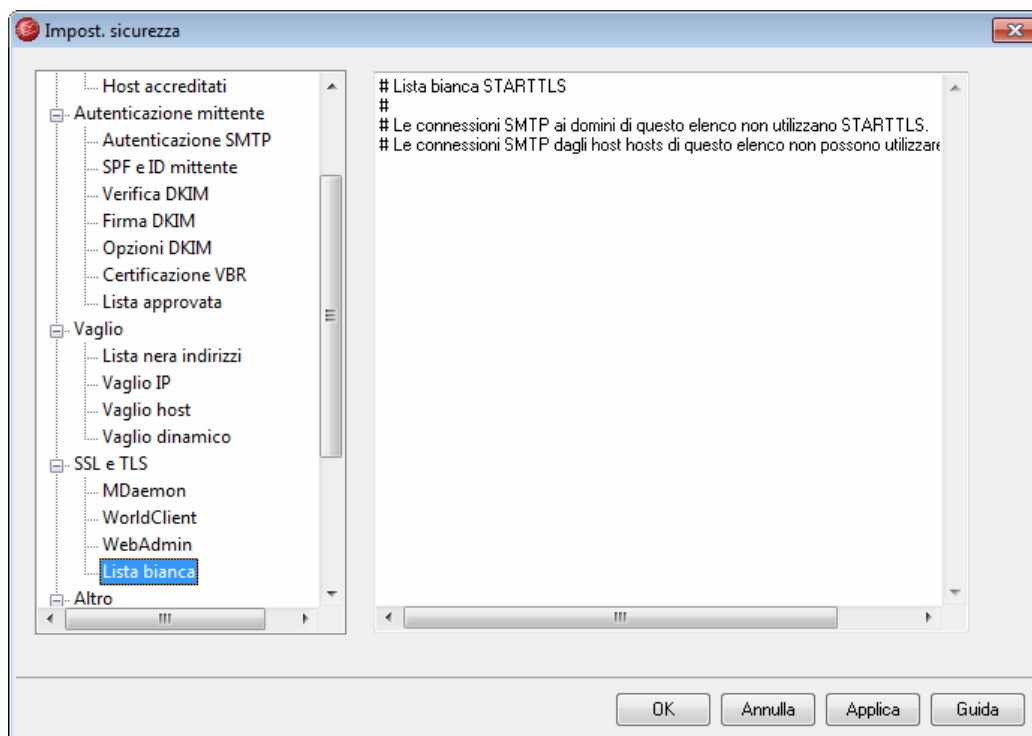
Riavvia server Web
Per riavviare il server Web, fare clic su questo pulsante. Per poter utilizzare i nuovi certificati, è necessario riavviare il server Web.

Per ulteriori informazioni sul protocollo SSL e sui certificati, vedere:

Esecuzione di WebAdmin con IIS 150
SSL e certificati 311
Creazione e uso dei certificati SSL 320

Per ulteriori informazioni su WebAdmin, vedere:

Configurazione remota 144
WebAdmin » Server Web 145
Valori predefiniti di accesso Web 382
Account Editor » Accesso Web 347

5.4.4.4 Lista bianca

Questa lista bianca consente di impedire l'utilizzo di STARTTLS per l'invio o la ricezione di posta da domini o host specifici.

5.4.4.5 Creazione e uso dei certificati SSL

Se la creazione di certificati avviene mediante la finestra di dialogo SSL & TLS, MDaemon genera certificati autofirmati. In altre parole, l'autorità emittente o CA (Certificate Authority, autorità di certificazione) coincide con il proprietario del

certificato. Si tratta di una procedura valida e consentita ma, poiché l'autorità di certificazione non è presente nell'elenco delle autorità accreditate, quando si esegue la connessione all'URL HTTPS di WorldClient o di WebAdmin viene richiesto se proseguire la connessione al sito e/o installare il certificato. Dopo aver dato la conferma per l'installazione del certificato e aver accreditato il dominio di WorldClient come CA valida, il messaggio dell'avviso di protezione non viene più visualizzato.

Quando si effettua una connessione a MDaemon attraverso un client di posta come Microsoft Outlook, non viene tuttavia offerta la possibilità di installare il certificato. È possibile scegliere se proseguire o meno nell'uso temporaneo del certificato, anche se non convalidato. Ogni volta che il client di posta viene avviato e si effettua una connessione al server, è necessario scegliere se continuare a utilizzare il certificato non convalidato. Per evitare ciò, è necessario esportare il certificato e distribuirlo agli utenti via e-mail o mediante altri mezzi. Gli utenti potranno quindi installare manualmente il certificato e accreditarlo per evitare eventuali messaggi di avviso.

Creazione di un certificato

Per creare un certificato da MDaemon, seguire le istruzioni descritte di seguito.

1. Passare alla finestra di dialogo SSL e TLS di MDaemon, facendo clic su Sicurezza » Impostazioni sicurezza » SSL e TLS » MDaemon.
2. Abilitare la casella "*Abilita SSL, STARTTLS e STLS*".
3. Nella casella denominata "*Nome host*", inserire il dominio al quale appartiene il certificato (ad esempio, "`posta.esempio.com`").
4. Inserire il nome dell'organizzazione o dell'azienda proprietaria del certificato nella casella di testo "*Nome organizzazione/azienda*".
5. In "*Nomi host alternativi*", inserire tutti gli altri nomi di dominio che verranno utilizzati dagli utenti per accedere al server (ad esempio, "`*.dominio.com`", "`esempio.com`", "`wc.altn.com`" e così via).
6. Scegliere la lunghezza della chiave crittografica dalla casella di riepilogo a discesa.
7. Selezionare il paese o la regione in cui si trova il server.
8. Fare clic su Crea certificato.

Uso di certificati emessi da un'altra autorità di certificazione

Se si è acquistato o creato un certificato con un'origine diversa da MDaemon, è possibile utilizzarlo importandolo tramite Microsoft Management Console nell'archivio certificati di MDaemon. A questo scopo, utilizzando Windows XP:

1. Nella barra degli strumenti di Windows, fare clic su **Start » Esegui** e inserire "**`mmc /a`**" nella casella di testo.

2. Fare clic su **OK.**

3. In Microsoft Management Console, fare clic su **File » Aggiungi/Rimuovi snap-in** nella barra dei menu o premere la combinazione di tasti **CTRL+M** della tastiera.

4. Nella scheda Autonomo, fare clic su **Aggiungi**

5. Nella finestra di dialogo *Aggiungi snap-in autonomo*, fare clic su **Certificati** e, quindi, su **Aggiungi.**

6. Nella finestra di dialogo *Snap-in certificati*, selezionare **Account del computer** e, quindi, fare clic su **Avanti.**

7. Nella finestra di dialogo *Selezione computer*, selezionare **Computer locale** e, quindi, fare clic su **Fine.**

8. Fare clic su **Chiudi** e, quindi, su **OK.**

9. In *Certificati (computer locale)* situato nel riquadro di sinistra, se il certificato da importare è autofirmato, fare clic su **Autorità di certificazione fonti attendibili** e, quindi, su **Certificati.** In caso contrario, fare clic su **Personale.**

10. Nella barra dei menu, fare clic su **Azione » Tutte le attività » Importa** e, quindi, su **Avanti.**

11. Inserire il percorso del file del certificato da importare, utilizzando il pulsante Sfoglia se necessario, quindi fare clic su **Avanti.**

12. Fare clic su **Avanti** e, quindi, su **Fine.**

MDaemon consente di visualizzare solo certificati con chiavi private che utilizzano il formato Personal Information Exchange (PKCS #12). Se il certificato importato non viene visualizzato nell'elenco, è necessario importare un file con estensione `PEM` che contiene sia la chiave del certificato che la chiave privata. Eseguendo l'importazione del file PEM con lo stesso processo descritto in precedenza, il file viene convertito automaticamente nel formato PKCS #12.

Vedere:

SSL e TLS 311

5.4.5 Altro

5.4.5.1 Protezione backscatter - Panoramica

Backscatter

Il termine "Backscatter" si riferisce ai messaggi di risposta ricevuti dagli utenti relativi a messaggi mai spediti. Ciò si verifica quando i messaggi spam o i messaggi inviati da virus includono un indirizzo di ritorno contraffatto. Di conseguenza, se uno di questi messaggi viene respinto dal server del destinatario o se all'account del destinatario è associata una risposta automatica relativa, ad esempio, all'assenza per vacanze o trasferimento, il messaggio di risposta viene diretto all'indirizzo contraffatto. Ciò provoca la ricezione di migliaia di messaggi fittizi relativi a notifiche dello stato di recapito, a vacanze o assenze, a risposte automatiche e così via. Gli spammer e i creatori di virus, inoltre, sfruttano spesso questo fenomeno e lo utilizzano per lanciare attacchi di tipo DoS (Denial of Service) contro i server di posta, determinando così la ricezione di innumerevoli messaggi e-mail non validi da server sparsi in tutto il mondo.

Soluzione di MDaemon

Per contrastare questo fenomeno, MDaemon include una funzionalità chiamata Protezione backscatter (BP, Backscatter Protection). Questa funzionalità utilizza un metodo di codifica hash di una chiave privata per generare e inserire nell'indirizzo del percorso di ritorno dei messaggi in uscita uno speciale codice con validità temporale limitata, in modo da consentire la ricezione dei soli messaggi di risposta automatica e di notifica di recapito legittimi. Quando uno di tali messaggi riscontra un problema di consegna e viene rispedito oppure quando viene ricevuto un messaggio di risposta automatica al quale è associato il percorso di ritorno "`mailer-daemon@...`" o `NULL`, MDaemon è in grado di individuare il codice speciale e di verificare che si tratta di una risposta automatica legittima a un messaggio spedito da uno degli account in uso. Se il messaggio include un indirizzo privo del codice speciale o se quest'ultimo ha più di sette giorni, l'evento viene registrato da MDaemon e il messaggio può essere rifiutato.

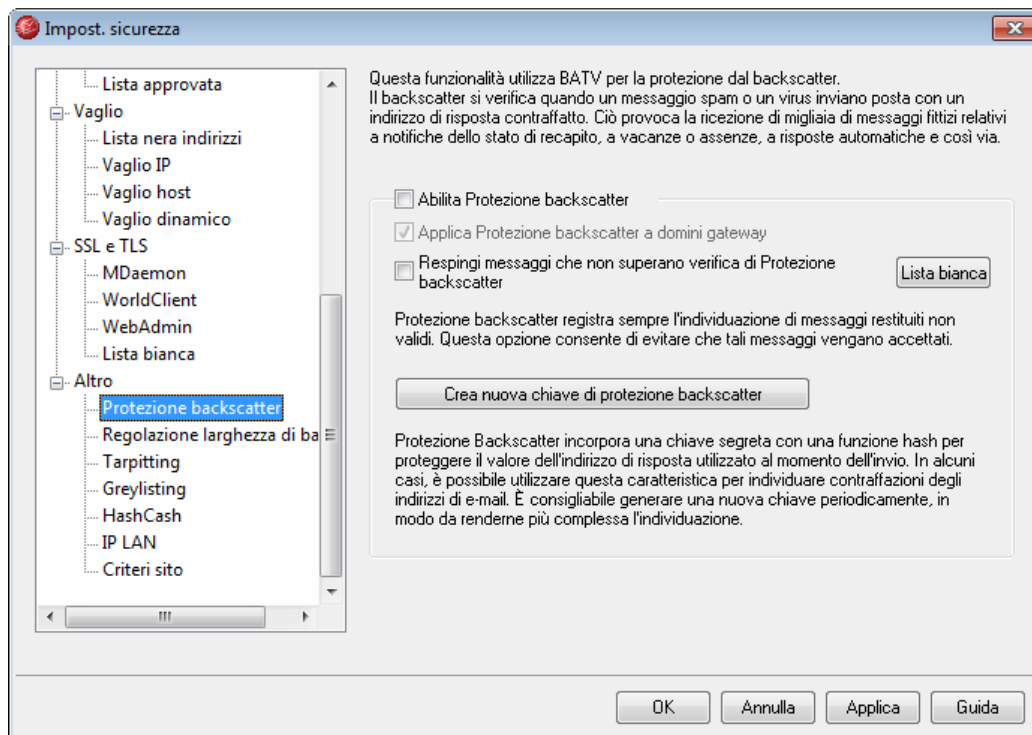
La funzione Protezione Backscatter324 è disponibile in: Sicurezza » Impostazioni sicurezza » Altro » Protezione backscatter.

La funzionalità Protezione backscatter è un'implementazione della convalida BATV (Bounce Address Tag Validation). Per ulteriori informazioni su BATV, visitare il sito

`http://www.mipassoc.org/batv/`

Per ulteriori informazioni, vedere:

Protezione backscatter 324

5.4.5.1.1 Protezione backscatter

Protezione backscatter

Abilita Protezione backscatter

Selezionare questa casella di controllo se si desidera inserire un codice speciale di Protezione backscatter nell'indirizzo "Return-Path" di ciascun messaggio. Il codice viene generato utilizzando la chiave privata inclusa nel file `rsa.private` che si trova nella cartella `PEM\_batv\` di MDaemon. Il codice è valido per sette giorni. I messaggi DSN in entrata o di risposta automatica, ai quali è associato il percorso di ritorno "`mailer-daemon@...`" o `NULL` devono includere un codice Protezione backscatter valido; in caso contrario, la convalida ha esito negativo.

Se l'opzione viene disabilitata, il codice speciale di Protezione backscatter non viene inserito nei messaggi in uscita. La funzionalità rimane attiva, tuttavia, per verificare che i messaggi di notifica dello stato del recapito e di risposta automatica che includono un codice valido non vengano erroneamente respinti.

Applica Protezione backscatter a domini gateway

Se la funzionalità protezione backscatter è attiva, questa opzione consente di applicarla anche ai domini per i quali MDaemon opera come gateway o server di backup. Per ulteriori informazioni, vedere Gateway di dominio 458.

Respingi messaggi che non superano la verifica di Protezione backscatter
Selezionare questa casella di controllo se si desidera rifiutare i messaggi di notifica dello stato del recapito o di risposta automatica che non superano la convalida di Protezione backscatter. I messaggi ai quali è associato il percorso di ritorno "`mailer-daemon@...`" o `NULL` non superano la verifica se sono privi del codice speciale o se quest'ultimo ha più di sette giorni. Grazie all'affidabilità della Protezione backscatter, non sono possibili falsi positivi né esistono aree di incertezza: un messaggio è valido oppure non lo è. È quindi possibile configurare MDaemon in modo che respinga i messaggi non validi, purché tutti i messaggi in uscita dagli account includano lo speciale codice di Protezione backscatter. Il risultato della verifica di Protezione backscatter viene sempre registrato nel file registro SMTP (entrata), anche se si sceglie di non respingere i messaggi che non superano la verifica. I messaggi in entrata relativi ai gateway non vengono respinti a meno che l'opzione *Applica Protezione backscatter a domini gateway* non sia stata selezionata.

Quando si abilita la funzionalità Protezione backscatter è opportuno attendere una settimana prima di attivare l'opzione che consente di scartare i messaggi di risposta automatica non validi. In questa finestra temporale, infatti, possono essere ricevuti messaggi di notifica dello stato del recapito o di risposta automatica inviati prima dell'attivazione di Protezione backscatter e attivando tale opzione alcuni messaggi di riposta legittimi potrebbero essere erroneamente respinti. Una settimana rappresenta un periodo di tempo ragionevole per l'attivazione dell'opzione di scarto dei messaggi non validi. Questa avvertenza è valida anche nel caso in cui si crei una nuova chiave di Protezione backscatter e si elimini immediatamente quella precedente, senza continuare a utilizzarla per una settimana. Per ulteriori informazioni, vedere l'opzione *Crea nuova chiave di protezione backscatter*.

Lista bianca
Fare clic su questo pulsante per aprire la lista bianca della Protezione backscatter. In questa lista è possibile indicare gli indirizzi IP o i domini che si desidera escludere dalla protezione backscatter.

Crea nuova chiave di protezione backscatter
Fare clic su questo pulsante per creare una nuova chiave di protezione backscatter. Questa chiave viene utilizzata da MDaemon per creare e verificare i codici speciali inseriti nei messaggi. La chiave è inclusa nel file `rsa.private` che si trova nella cartella `PEM\_batv\` di MDaemon. Quando viene generata la nuova chiave, una finestra di messaggio segnala che la chiave precedente rimane operativa per sette giorni, a meno che non la si elimini immediatamente. Nella maggior parte dei casi è opportuno scegliere "**No**" e continuare a utilizzare la chiave per altri sette giorni. Se la chiave viene eliminata immediatamente, la verifica di alcuni dei messaggi legittimi in entrata potrebbe avere esito negativo perché rappresentano risposte a messaggi che includono il codice speciale generato dalla chiave precedente.

Se il traffico e-mail è suddiviso tra più server, è possibile che il file contenente la chiave debba essere condiviso da tutti i server o da tutti gli MTA (Mail Transfer Agent) in uso.

Vedere:

Protezione backscatter - Panoramica 323

5.4.5.2 Regolazione larghezza di banda - Panoramica

La funzionalità di regolazione della larghezza di banda è una nuova funzione che consente di controllare la larghezza di banda utilizzata da MDaemon. È possibile controllare la velocità di avanzamento delle sessioni o dei servizi impostando velocità diverse per ogni servizio principale di MDaemon in base al dominio, compresi il dominio predefinito, i domini aggiuntivi e i gateway di dominio. È inoltre possibile impostare i limiti per le connessioni locali selezionando "Traffico locale" in una casella a discesa. In questo modo, possono essere create particolari impostazioni per la larghezza di banda, che verranno applicate se la connessione ha origine o fine in un indirizzo IP locale o in un nome di dominio.

La funzione di regolazione della larghezza di banda può essere applicata sia in base alla sessione, sia in base al servizio. Se la funzione è applicata in base alla sessione, la velocità di ogni sessione viene regolata indipendentemente dalle altre. Di conseguenza, più sessioni dello stesso tipo di servizio attive contemporaneamente possono superare il valore impostato per il servizio. Quando si configura la regolazione della larghezza di banda in base al servizio, MDaemon controlla l'utilizzo complessivo delle sessioni relative allo stesso tipo di servizio e suddivide equamente la larghezza di banda totale. Più sessioni quindi condividono equamente la larghezza di banda massima configurata. Questo consente di impostare un limite per l'intero servizio.

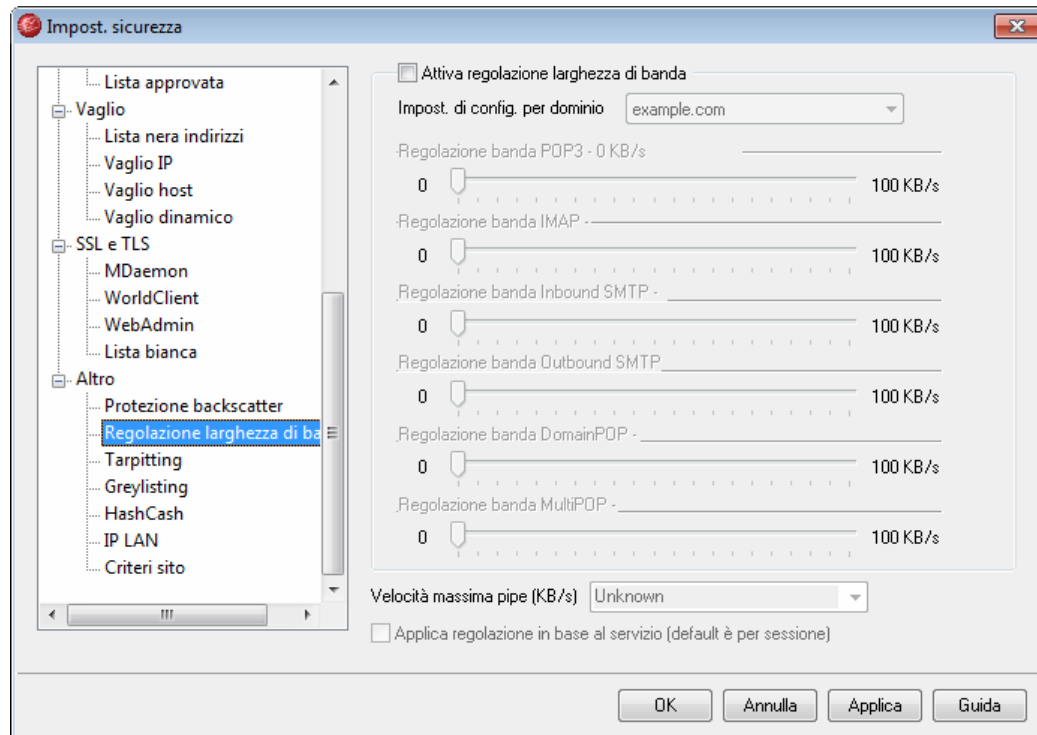
Quando si estende la funzione Regolazione larghezza di banda a un gateway di dominio, è necessario gestire il gateway in modo leggermente diverso dal solito, in quanto a questo non è associato un indirizzo IP. Per determinare se al gateway sia associata la sessione SMTP in entrata, MDaemon deve utilizzare il valore passato al comando RCPT. In caso affermativo, alla sessione SMTP in entrata viene applicata la regolazione della larghezza di banda. A causa dei limiti di SMTP, se uno dei destinatari di un messaggio è rappresentato da un gateway di dominio, la regolazione della larghezza di banda viene applicata all'intera sessione.

Il sistema Regolazione larghezza di banda opera in termini di kilobyte al secondo (KB/s). Il valore "0", indicando che non è previsto alcun limite alla velocità di avanzamento della sessione o del servizio, consente l'utilizzo della massima larghezza di banda disponibile. Il valore "10", ad esempio, impone a MDaemon di regolare la velocità di trasmissione in modo che questa si attesti su un valore uguale o leggermente superiore a 10 KB/s.

Gli impulsi di attività all'inizio di una sessione possono superare i limiti fissati. La regolazione ha luogo e diventa più precisa durante l'avanzamento della sessione.

Per ulteriori informazioni, vedere:

[Regolazione larghezza di banda](327)
[IP LAN](336)

5.4.5.2.1 Regolazione larghezza di banda

Attiva regolazione larghezza di banda
Questa casella di controllo consente di attivare la funzione Regolazione larghezza di banda.

Impost. di config. per dominio
Selezionare un dominio nell'elenco a discesa e impostare le opzioni relative ai vari servizi per configurare la regolazione della larghezza di banda del dominio selezionato. L'impostazione di un particolare controllo su "0" indica che per la larghezza di banda di quel tipo di servizio non è previsto alcun limite. L'ultima voce dell'elenco a discesa è *Local Traffic (Traffico locale)*. Impostando la regolazione della larghezza di banda per questa opzione, si determina un limite per il traffico locale, ovvero per le sessioni e i servizi che utilizzano la LAN locale. La schermata IP LAN 336 consente di indicare l'elenco dei domini e degli indirizzi IP da considerare locali.

Servizi

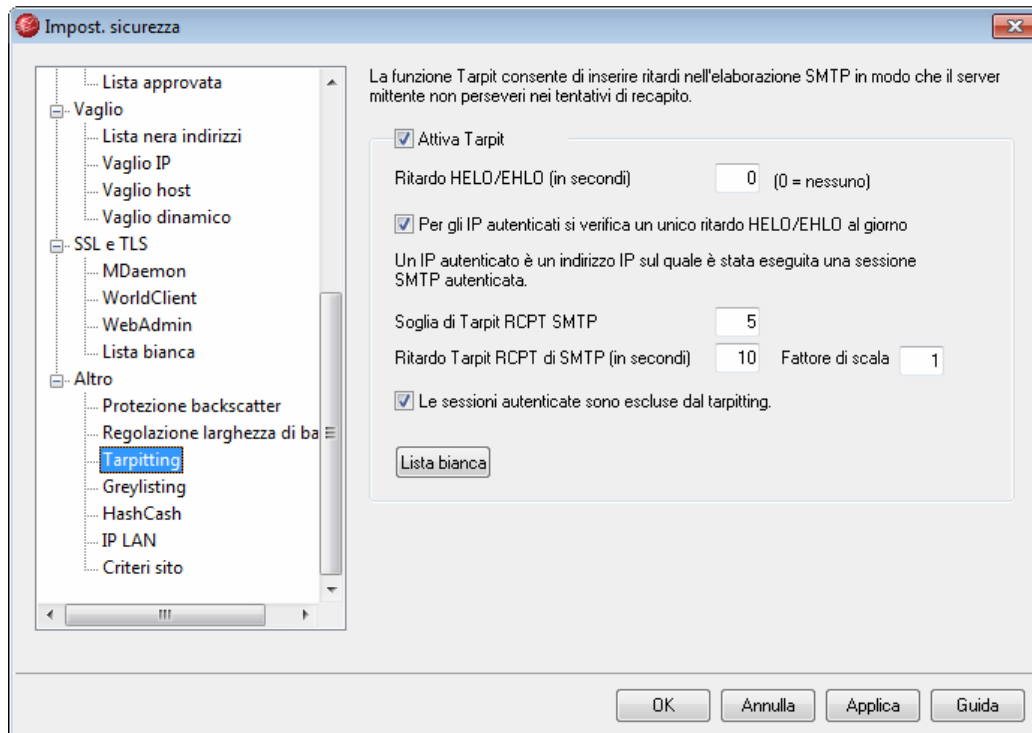
Regolazione della larghezza di banda - [tipo di servizio] - XX KB/s
Dopo aver selezionato un dominio nell'elenco a discesa, è possibile utilizzare questi

controlli per impostare un limite alla larghezza di banda del dominio selezionato. L'impostazione del valore "0" indica che non è previsto alcun limite per la larghezza di banda del particolare tipo di servizio. Scegliendo un numero diverso da zero, si imposta un limite sulla larghezza di banda, in kilobyte al secondo, per il servizio selezionato.

Velocità massima pipe (KB/s)
Scegliere la velocità massima di connessione, in kilobyte al secondo, dall'elenco a discesa.

Applica regolazione in base al servizio (default è per sessione)
Abilitare questa casella di controllo se si desidera applicare la regolazione della larghezza di banda in base al servizio anziché la sessione, secondo l'impostazione predefinita. Quando la regolazione è impostata in base al servizio, la quantità di larghezza di banda allocata viene suddivisa equamente tra tutte le sessioni attive di quel tipo di servizio. Di conseguenza, la quantità totale di larghezza di banda utilizzata, ad esempio, da più client IMAP connessi contemporaneamente non può mai superare la quantità indicata, indipendentemente dal numero dei client connessi. Se la regolazione è impostata in base alla *sessione*, il limite indicato non può essere superato da una singola sessione IMAP, ma solo dal totale di più sessioni attive contemporaneamente.

Per ulteriori informazioni, vedere:

Regolazione larghezza di banda - Panoramica 326

5.4.5.3 Tarpitting

La funzione Tarpitting è disponibile in: Sicurezza » Impostazioni sicurezza » Altro » Tarpitting.

Questa funzione consente di rallentare deliberatamente una connessione a seguito della ricezione di un determinato numero di comandi RCPT dal mittente. Ciò consente di scoraggiare l'utilizzo del server da parte di coloro che inviano messaggi di posta elettronica indesiderati ("spam"). È possibile specificare il numero di comandi RCPT consentiti prima dell'inizio del tarpitting e il numero di secondi di ritardo della connessione ogni volta che si riceve il successivo comando dall'host. L'assunto che sottende a questa tecnica consiste nell'imporre ai mittenti di messaggi indesiderati un periodo di attesa lungo e variabile per l'invio di ogni messaggio, scoraggiandoli così a riutilizzare in futuro il server per questa operazione.

Attiva Tarpit
Per attivare le funzionalità Tarpit di MDaemon, selezionare questa casella di controllo.

Ritardo HELO/EHLO (in secondi)
Utilizzare questa opzione per ritardare la risposta del server ai comandi SMTP EHLO/HELO. Un ritardo di risposta pari anche a solo dieci secondi consente di ridurre significativamente il tempo di elaborazione grazie alla riduzione della posta spam ricevuta. Spesso, gli spammer fanno affidamento sulla consegna rapida dei messaggi e pertanto non attendono a lungo una risposta ai comandi EHLO/HELO. Con un ritardo anche minimo, gli strumenti di spam spesso desistono e proseguono con altre attività invece di attendere una risposta. Le connessioni sulla porta MSA, specificata nella scheda Porte 49 di Dominio predefinito/server 40, vengono sempre escluse da

questo ritardo. L'impostazione predefinita di questa opzione è pari a "0" e indica che i comandi `EHLO`/`HELO` non verranno ritardati.

Per gli IP autenticati si verifica un solo ritardo HELO/EHLO al giorno
Selezionare questa casella di controllo se si desidera applicare il ritardo EHLO/HELO una sola volta al giorno nel caso di sessioni autenticate provenienti da specifici indirizzi IP. Il ritardo verrà applicato al primo messaggio proveniente dall'indirizzo IP, ma tutti i messaggi successivi provenienti dallo stesso indirizzo IP non subiranno ritardi.

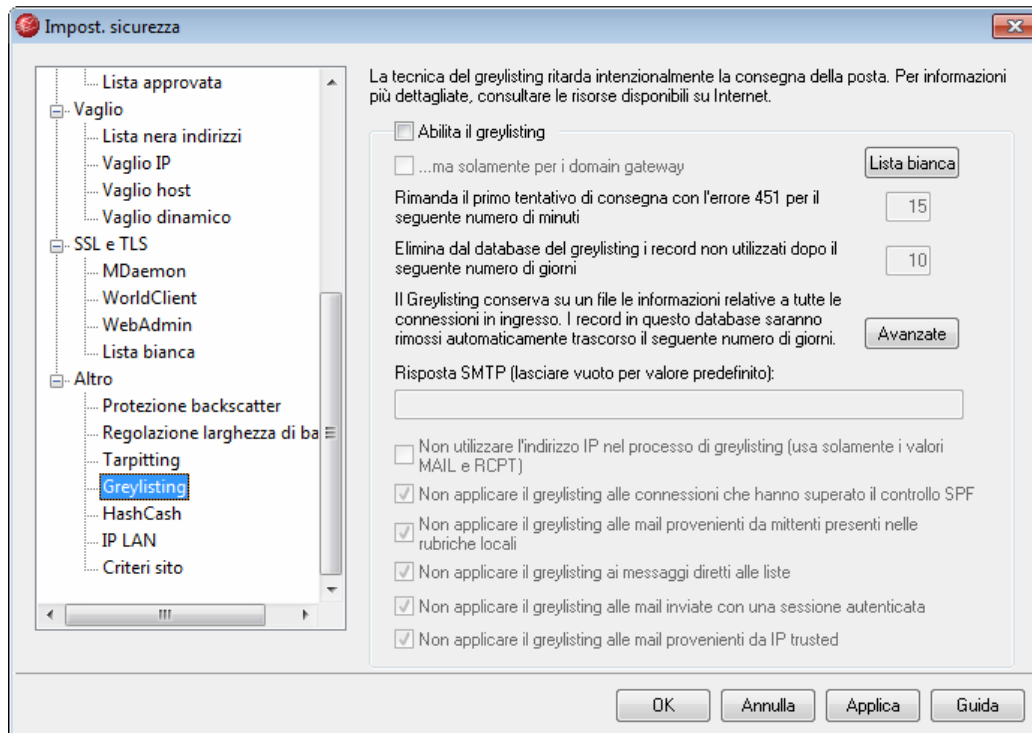
Soglia di Tarpit RCPT SMTP
Indicare il numero di comandi `RCPT` del protocollo SMTP consentiti in una sessione di posta prima che MDaemon attivi il tarpitting dell'host. Ad esempio, se si imposta il valore 10 e l'host mittente tenta di inviare un messaggio a 20 indirizzi (ossia utilizza 20 comandi `RCPT`), MDaemon consentirà il normale invio per i primi 10 indirizzi e si interromperà dopo ogni comando successivo per il numero di secondi specificato nella casella *Ritardo Tarpit RCPT di SMTP*.

Ritardo Tarpit RCPT di SMTP (in secondi)
Quando viene raggiunto il valore indicato per l'host nel campo *Soglia di Tarpit RCPT SMTP*, MDaemon rimarrà in attesa per il numero di secondi indicato in questo campo dopo la ricezione di ogni successivo comando `RCPT` inviato dall'host durante la sessione di posta.

Fattore di scala
Rappresenta il coefficiente in base al quale aumenta il ritardo tarpit nel tempo. Una volta raggiunta la soglia tarpit e applicato alla sessione il ritardo tarpit, la durata del successivo ritardo nella sessione viene determinata moltiplicando questo coefficiente per la durata del ritardo precedente. Ad esempio, se il ritardo tarpit è impostato su 10 e il fattore di scala su 1,5, il primo ritardo sarà di 10 secondi, il secondo di 15, il terzo di 22,5 e il quarto di 33,75, poiché 10 x 1,5 = 15; 15 x 1,5 = 22,5 e così via. Il valore predefinito del fattore di scala è 1 e indica che il ritardo non viene incrementato.

Le sessioni autenticate sono escluse dal tarpitting
Selezionando questa casella di controllo, i mittenti che autenticano le sessioni non vengono interessati dalla funzione di Tarpitting.

Lista bianca
Fare clic su questo pulsante per aprire la finestra di dialogo Lista bianca all'interno della quale è possibile inserire gli indirizzi IP che si desidera escludere dalla funzione di Tarpitting.

5.4.5.4 Greylisting

La funzione Greylisting è disponibile nella finestra di dialogo Sicurezza, in: Sicurezza » Impostazioni sicurezza » Altro » Greylisting. Il Greylisting è una tecnica antispam che sfrutta il fatto che i server SMTP ritentano la consegna di qualsiasi messaggio riceva un codice di errore temporaneo del tipo "riprovare più tardi". Utilizzando questa tecnica, durante la sessione SMTP i messaggi che provengono da un mittente non inserito nella lista bianca o semplicemente sconosciuto vengono rifiutati con un codice di errore temporaneo e gli indirizzi IP del mittente, del destinatario e del server di invio vengono registrati. Ogni successivo tentativo di consegna verrà temporaneamente rifiutato per un intervallo di tempo prestabilito (ad esempio 15 minuti). Dal momento che gli "spammer" in genere non eseguono ulteriori tentativi di consegna una volta che un messaggio viene rifiutato, questa funzione consente di ridurre considerevolmente il numero di messaggi spam ricevuti. Qualora uno "spammer" ritenti la consegna in un secondo momento, inoltre, è possibile che sia già stato identificato e che altre funzioni antispam, ad esempio l'inserimento nelle Liste nere DNS 267, siano in grado di bloccarlo. È importante sottolineare, tuttavia, che questa tecnica può ritardare il ricevimento di posta "non spam" insieme a quella indesiderata. I messaggi considerati legittimi vengono comunque consegnati una volta scaduto il periodo di tempo stabilito per il greylisting. È importante anche sottolineare che non esiste un modo per determinare i tempi di attesa dei server di invio prima di ulteriori tentativi di consegna. È possibile che il rifiuto di messaggi con un codice di errore temporaneo determini ritardi di durata indeterminata, compresa tra pochi minuti e un'intera giornata.

Esistono numerosi problemi comuni ed effetti collaterali negativi associati al greylisting. La schermata Greylisting offre una serie di opzioni che consentono di gestire tali problemi.

In primo luogo, per l'invio della posta in uscita alcuni domini utilizzano un insieme di

server. Poiché ogni tentativo di consegna può essere effettuato da un server differente, la funzione greylisting considererebbe ogni tentativo come una nuova connessione. Ciò potrebbe aumentare il tempo impiegato per superare il blocco applicato da questa funzione, perché ogni tentativo verrebbe considerato come un messaggio diverso anziché un nuovo tentativo di consegna di un messaggio precedente. Utilizzando un'opzione di ricerca SPF, nel caso di domini di invio che pubblicano i propri dati SPF questo problema può essere risolto. Esiste inoltre un'opzione che consente di ignorare completamente l'indirizzo IP del server di posta. L'utilizzo di questa opzione riduce l'efficienza della funzione greylisting, ma risolve completamente i problemi legati all'invio da server differenti.

In secondo luogo, la funzione greylisting richiede generalmente un database di grandi dimensioni poiché è necessario tenere traccia di ogni connessione in entrata. In MDaemon, la quantità di connessioni di cui tenere traccia è ridotta perché la funzione Greylisting viene applicata in prossimità della fine della sequenza di elaborazione SMTP. Ciò consente di applicare al messaggio tutte le altre opzioni di filtro di MDaemon prima che questo raggiunga la fase di greylisting. Di conseguenza, le dimensioni del file dati per la funzione greylisting vengono significativamente diminuite. Poiché tale file è residente in memoria, inoltre, l'impatto sulle prestazioni è minimo.

Infine, sono disponibili numerose opzioni che consentono di ridurre l'impatto della funzione greylisting sui messaggi "non spam". Innanzitutto, è possibile escludere i messaggi inviati alle liste di distribuzione. Inoltre, questa opzione dispone di un proprio file di lista bianca nel quale è possibile definire gli indirizzi IP, i mittenti e i destinatari che si desidera escludere dalla funzione greylisting. Infine, è disponibile un'opzione che consente di utilizzare i file della rubrica privata di ciascun account come database della lista bianca. È quindi possibile escludere dalla funzione greylisting la posta proveniente da utenti contenuti nella rubrica.

Per ulteriori informazioni generali sulla funzione Greylisting, visitare il sito Internet di Even Harris all'indirizzo:

http://projects.puremagic.com/greylisting/.

Greylisting

Abilita il greylisting
Selezionare questa opzione per attivare la funzione Greylisting.

...ma solamente per i domain gateway
Selezionare questa opzione se si desidera attivare la funzione solo per i messaggi destinati a domini gateway.

Lista bianca
Questo pulsante consente di aprire la lista bianca nella quale definire i mittenti, i destinatari e gli indirizzi IP che verranno esclusi dalla funzione Greylisting.

Rimanda il primo tentativo di consegna con l'errore 451 per il seguente numero di minuti
Consente di definire per quanti minuti un tentativo di consegna deve rimanere bloccato dopo il tentativo iniziale. Durante questo intervallo, ogni successivo tentativo di consegna eseguito dalla stessa combinazione server/mittente/ destinatario (definita anche come "tripletta Greylist") verrà rifiutato con un altro codice di errore temporaneo. Una volta scaduto l'intervallo di tempo, per la tripletta

non verrà implementato alcun ulteriore ritardo a meno che il record di database corrispondente non sia stato eliminato perché scaduto.

Elimina dal database del greylisting i record non utilizzati dopo il seguente numero di giorni
Una volta scaduto il periodo iniziale per una determinata tripletta, ai successivi messaggi relativi alla stessa tripletta non verranno applicati altri ritardi. Tuttavia, se non viene ricevuto alcun messaggio corrispondente alla tripletta per il numero di giorni indicato in questa opzione, il relativo record di database viene eliminato. I tentativi di consegna successivi eseguiti dalla stessa tripletta generano un nuovo record e, di conseguenza, il periodo di ritardo iniziale viene applicato nuovamente.

Avanzate
Fare clic su questo pulsante per aprire il database Greylisting e rivedere o modificare le triplette.

Risposta SMTP (lasciare vuoto per valore predefinito)
Se si inserisce una stringa di testo personalizzata, MDaemon restituisce la risposta SMTP "`451 <testo personalizzato>`", anziché il messaggio predefinito "`Greylisting abilitato. Riprovare tra X minuti`." Questa funzione è utile, ad esempio, per indicare una stringa contenente un URL che fa riferimento a una descrizione della tecnologia greylisting.

Non utilizzare l'indirizzo IP nel processo di greylisting (usa solamente i valori MAIL e RCPT)
Selezionare questa casella di controllo se non si desidera utilizzare l'indirizzo IP del server di invio come parametro per la funzione greylisting. Ciò consente di risolvere eventuali problemi causati dagli insiemi di server, ma riduce le prestazioni della funzione Greylisting.

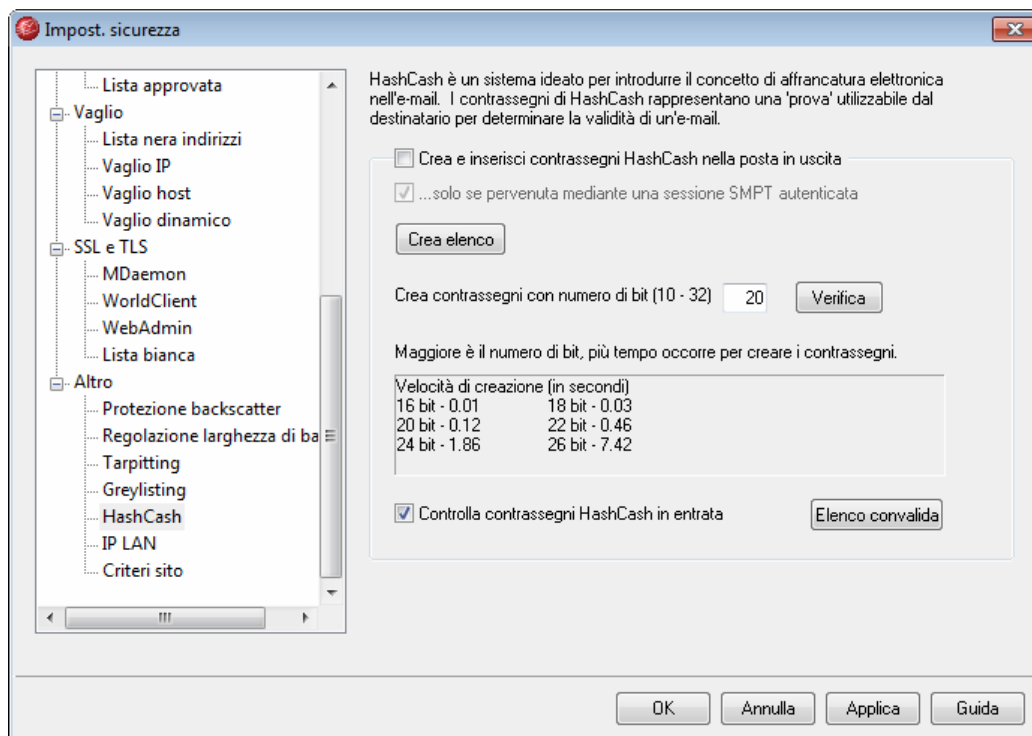
Non applicare il greylisting alle connessioni che hanno superato il controllo SPF
Quando si utilizza questa opzione, se un messaggio in arrivo corrisponde al mittente e al destinatario di una tripletta ma non al server di invio e se l'elaborazione SPF indica quest'ultimo come un'alternativa valida a quello elencato nella tripletta , il messaggio viene gestito come fosse una consegna successiva relativa alla stessa tripletta anziché come una nuova connessione per cui creare un nuovo record Greylisting.

Non applicare il greylisting alle mail provenienti da mittenti presenti nelle rubriche locali
Selezionare questa casella di controllo se si desidera escludere un messaggio dalla funzione Greylisting quando il mittente è presente nella rubrica del destinatario.

Non applicare il greylisting ai messaggi diretti alle liste
Selezionare questa casella di controllo se si desidera escludere dalla funzione Greylisting i messaggi delle liste di distribuzione.

Non applicare il greylisting alle mail inviate con una sessione autenticata
Utilizzare questa opzione se si desidera escludere dalla funzione Greylisting tutti i messaggi in arrivo durante una sessione autenticata.

Non applicare il greylisting alle mail provenienti da IP trusted
Utilizzare questa opzione se si desidera escludere dalla funzione Greylisting tutti i messaggi provenienti da indirizzi IP accreditati.

5.4.5.5 HashCash

HashCash è un sistema basato su "prove" e può essere considerato sia uno strumento antispam sia una contromisura contro attacchi di tipo DoS (Denial-of-Service), concettualmente analogo a un metodo di affrancatura elettronica. Grazie al sistema HashCash, MDaemon è in grado di "coniare" dei contrassegni HashCash, per i quali, in realtà, si "paga" in tempi di elaborazione della CPU anziché in moneta. Il contrassegno HashCash viene inserito nelle intestazioni dei messaggi in uscita e poi verificato dal server e-mail del destinatario e stimato in base al valore del contrassegno. La probabilità che i messaggi contrassegnati siano legittimi è maggiore, per questo tali messaggi possono superare i sistemi antispam del server ricevente. L'uso dei contrassegni HashCash consente di ridurre il numero di falsi positivi evitando così che vengano rifiutati qualora non superino i sistemi di blocco basati su liste nere o sulle parole contenute.

Gli "spammer" contano sulla capacità di inviare molte centinaia o addirittura centinaia di migliaia di messaggi in tempi estremamente brevi, inviando spesso una sola copia a più destinatari mediante la tecnica BCC (Copia nascosta) o altre analoghe che in generale non richiedono tempi di elaborazione eccessivi per i destinatari. Uno spammer che tenti di utilizzare un sistema HashCash, tuttavia, dovrebbe creare un contrassegno HashCash differente per ciascun destinatario ogni volta che al destinatario viene inviato un messaggio e ciò sarebbe proibitivo per uno "spammer" comune. Al contrario,

per un qualsiasi server o mittente di posta legittimi, i tempi extra richiesti dalla CPU per contrassegnare i messaggi in uscita risultano sostanzialmente poco significativi e non condizionano in modo rilevante la velocità di consegna della posta o i tempi di elaborazione, soprattutto perché i messaggi in uscita delle liste di distribuzione non sono mai contrassegnati.

I contrassegni vengono generati solo per i messaggi remoti in uscita provenienti o destinati agli indirizzi specificati nell'Elenco zecche e mai per i messaggi delle liste di distribuzione. Inoltre, per impostazione predefinita, MDaemon genera contrassegni HashCash solo quando il messaggio arriva mediante una sessione SMTP autenticata. È consigliato, ma non obbligatorio, richiedere sessioni autenticate. È possibile disattivare questa richiesta se si desidera contrassegnare i messaggi in arrivo in sessioni non autenticate.

Per i messaggi in arrivo, viene controllata solo la validità dei contrassegni contenuti nei messaggi destinati agli indirizzi specificati nell'Elenco convalida. Se un messaggio in arrivo contiene un contrassegno HashCash ma il destinatario non è presente nell'elenco, il contrassegno viene ignorato e il messaggio viene elaborato normalmente come se non contenesse alcun contrassegno HashCash. Per impostazione predefinita, questo elenco contiene solo il dominio predefinito. Fare clic sul pulsante *Elenco convalida* se si desidera aggiungere domini aggiuntivi o gateway di dominio.

Per ulteriori informazioni su HashCash, visitare l'indirizzo http://www.hashcash.org/.

HashCash

Crea e inserisci contrassegni HashCash nella posta in uscita
Per attivare il sistema HashCash, selezionare questa casella di controllo. MDaemon genera contrassegni per i messaggi remoti in uscita provenienti o destinati agli indirizzi specificati nell'elenco zecche.

... solo se pervenuta mediante una sessione SMTP autenticata
Fare clic su questa casella di controllo se si desidera generare solo contrassegni per i messaggi in arrivo mediante sessioni SMTP autenticate. È possibile, benché sconsigliato, deselezionare questa opzione se non si desidera richiedere l'autenticazione.

Crea elenco
Per aprire l'elenco delle zecche, fare clic su questo pulsante. MDaemon genera i contrassegni HashCash solo per gli indirizzi presenti in questo elenco. Per impostazione predefinita, questo elenco contiene solo il dominio predefinito. Se si desidera generare contrassegni per i domini aggiuntivi, per i gateway di dominio o per i messaggi destinati o provenienti da determinati utenti, è necessario aggiungere questi indirizzi all'elenco.

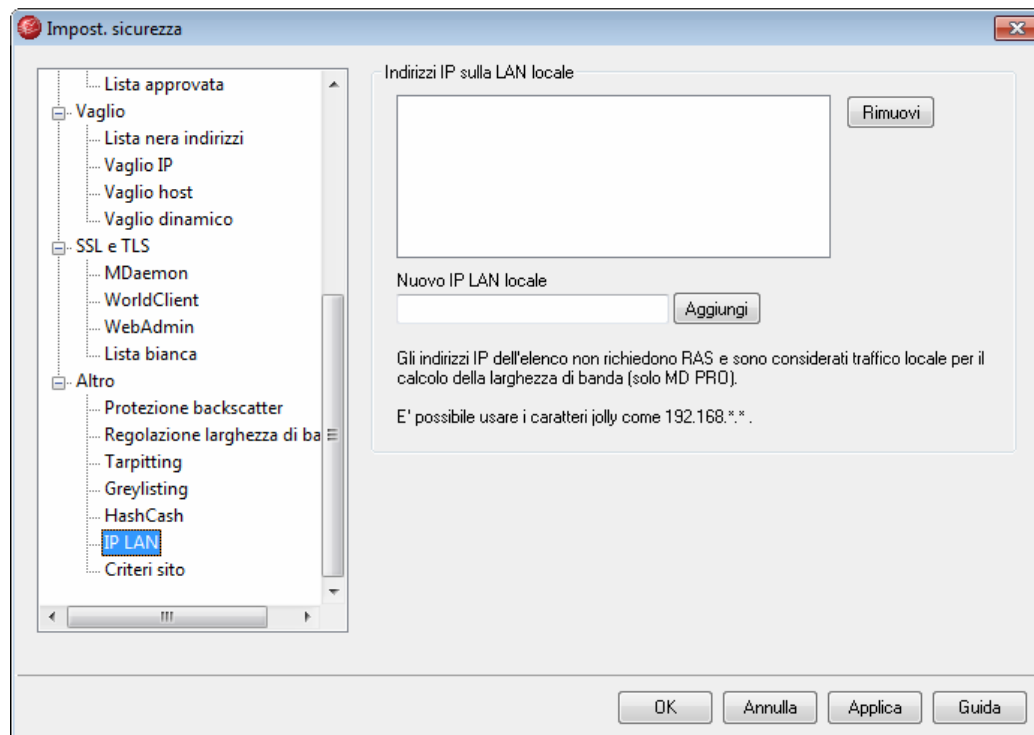
Crea contrassegni con numero di bit (10 -32)
Il valore associato a questo campo corrisponde al numero di bit che MDaemon usa quando genera contrassegni HashCash. Maggiore è il numero di bit, maggiore sarà il tempo di elaborazione richiesto per generare un contrassegno.

Verifica
Fare clic su questo pulsante per verificare la quantità di tempo necessaria a

generare un contrassegno con il numero di bit specificato.

Controlla contrassegni HashCash in entrata
Attivare questa opzione se si desidera controllare nei messaggi in entrata i contrassegni HashCash e modificare i punteggi di spam in base ai risultati. Verranno controllati solo i messaggi i cui destinatari sono contenuti nell'Elenco convalida. Se un messaggio in arrivo contiene un contrassegno HashCash ma il destinatario non è presente nell'elenco, il contrassegno viene ignorato e il messaggio viene elaborato normalmente come se non contenesse alcun contrassegno HashCash.

Elenco convalida
MDaemon tenta di convalidare solo i contrassegni HashCash dei messaggi i cui destinatari sono contenuti nell'Elenco convalida, mentre i messaggi in arrivo, i cui destinatari non sono presenti nell'elenco, vengono elaborati normalmente. Non viene effettuato alcun controllo sui contrassegni HashCash. Per impostazione predefinita, questo elenco contiene solo il dominio predefinito.

5.4.5.6 Indirizzi IP LAN

Nota: questa schermata è identica alla schermata omonima che si trova in Impostazioni di connessione RAS 100. Le modifiche apportate alle impostazioni in questa schermata verranno riportate anche nell'altra.

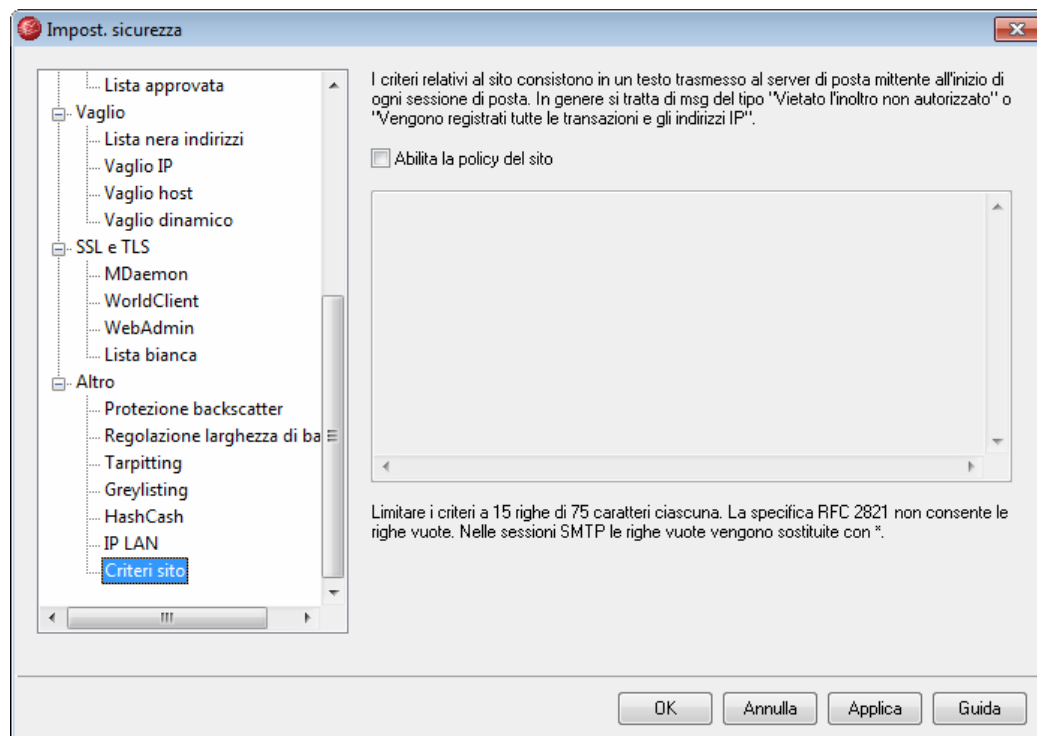
Indirizzi IP sulla LAN locale
In questa scheda vengono elencati gli indirizzi IP presenti sulla rete LAN locale. Questi

indirizzi non richiedono una connessione Internet e sono quindi considerati come "traffico locale" ai fini della limitazione della larghezza di banda. Agli indirizzi locali non vengono inoltre applicate numerose limitazioni relative al blocco della posta spam e alla sicurezza.

Rimuovi
Selezionare un indirizzo IP nell'elenco, quindi fare clic su questo pulsante per rimuoverlo. Lo stesso risultato può essere ottenuto facendo doppio clic sulla voce.

Nuovo IP LAN locale
Immettere un indirizzo IP da aggiungere all'elenco degli indirizzi IP locali, quindi fare clic su *Aggiungi*. È possibile utilizzare i caratteri jolly, ad esempio "127.0.*.*".

Aggiungi
Dopo aver immesso un indirizzo IP nel campo *Nuovo IP LAN locale*, fare clic su questo pulsante per aggiungerlo all'elenco.

5.4.5.7 Criteri sito

Creazione di un'informativa relativa alla protezione delle sessioni SMTP
Questa finestra di dialogo consente di specificare un'informativa relativa ai criteri di utilizzo (policy) del sito. Il testo viene memorizzato nel file `policy.dat`, situato nella sottodirectory `\app\` di MDaemon, per poi essere trasmesso ai server di invio all'inizio di ogni sessione di posta SMTP. Alcuni esempi di criteri di utilizzo del sito sono: "`Questo server non esegue l'inoltro`" oppure "`È vietato l'uso non autorizzato`". Non è necessario inserire all'inizio di ciascuna riga "`220`" o "

220-". MDaemon gestisce di conseguenza ciascuna riga, con o senza il prefisso relativo ai codici..

Durante la transazione SMTP, un'informativa relativa ai criterio di utilizzo del sito contenente un'istruzione relativa alla consegna della posta potrebbe avere l'aspetto seguente:

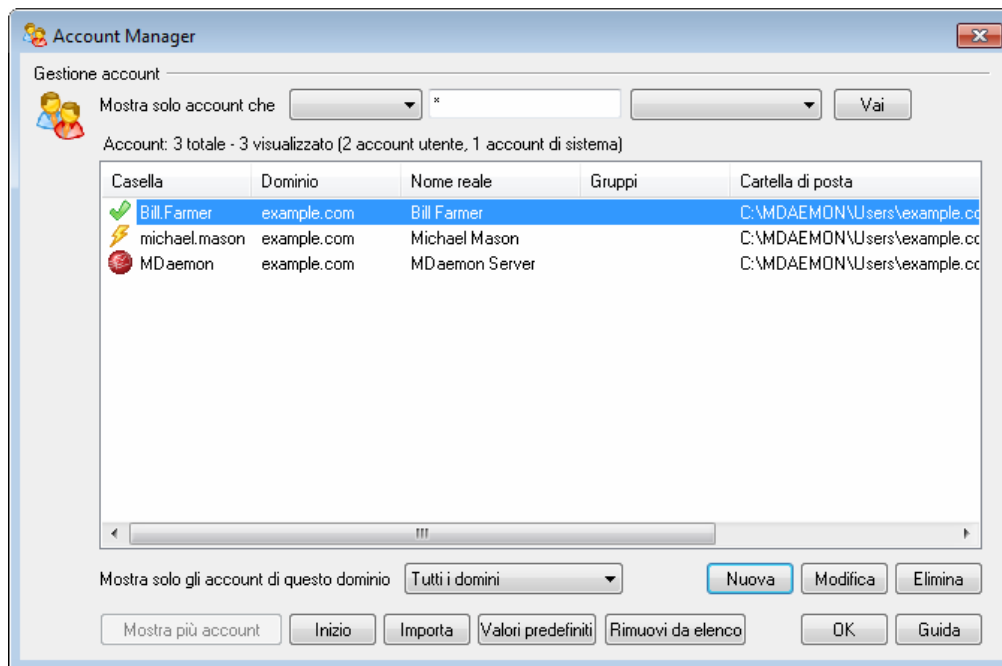
```
220-Alt-N Technologies ESMTP MDaemon
220-Questo sito non inoltra posta non autorizzata.
220-Agli utenti del server non autorizzati
220-non è consentito consegnare posta attraverso questo sito.
220
HELO domain.com
```

Il file POLICY.DAT deve essere composto solo da testo ASCII stampabile e non deve superare i 512 caratteri per riga. Tuttavia, è consigliabile non superare mai i 75 caratteri per riga. Questo file può avere la dimensione massima di 5.000 byte. MDaemon non visualizzerà file la cui dimensione superi i 5.000 byte.

Sezione VI

6 Menu Account

6.1 Account Manager

Per gestire al meglio la selezione, l'aggiunta, l'eliminazione o la modifica degli account, MDaemon offre lo strumento Account Manager. Questa finestra di dialogo fornisce l'accesso alle informazioni sugli account e può essere utilizzata per ordinarli in base alla casella postale, al dominio, al nome reale o alla cartella di posta. Account Manager è disponibile in: Account » Account Manager

Gestione degli account

Nella parte superiore dell'elenco degli account vengono visualizzate due statistiche relative all'elenco. Il primo dato indica il numero totale di account utente di MDaemon attualmente esistenti nel sistema. Il secondo dato rappresenta il numero degli account attualmente visualizzati nell'elenco. Gli account visualizzati dipendono dalla selezione effettuata nell'opzione *Mostra solo gli account di questo dominio* situata sotto l'elenco. Se è stata selezionata l'opzione "Tutti i domini", nell'elenco vengono visualizzati tutti gli account di MDaemon. Nella parte superiore della finestra di dialogo è presente un'opzione di ricerca che consente di definire esattamente gli account da visualizzare, non solo in base al dominio al quale appartengono.

Per ogni voce dell'elenco esiste un'icona relativa allo stato dell'account (vedere di seguito), la casella postale, il dominio al quale l'account appartiene, il "nome reale" del titolare dell'account, eventuali gruppi di appartenenza e la cartella di posta in cui sono memorizzati i messaggi dell'account. L'elenco può essere organizzato in ordine ascendente o discendente in base a qualsiasi colonna. Fare clic su un'intestazione di colonna per applicare all'elenco l'ordine ascendente in base a tale colonna. Fare di nuovo clic sulla colonna per applicare l'ordine discendente.

Per impostazione predefinita, l'elenco visualizza solo 500 account per volta. Se si desidera visualizzare un numero maggiore di account per il dominio selezionato (oppure per tutti i domini, se è stata selezionata l'opzione Tutti i domini), fare clic sul pulsante *Mostra più account* in modo da visualizzare i 500 account successivi. Per poter visualizzare più di 500 account per volta, aprire il file `MDaemon.ini` e modificare la chiave `MaxAccountManagerEntries=500` impostando il valore desiderato.

Icone di stato dell'account

L'account è un amministratore globale o di dominio.

Account con accesso completo. Sono abilitati sia gli accessi POP che IMAP.

Account con accesso limitato. È abilitato solo l'accesso POP o quello IMAP.

Account con accesso limitato. Sono disabilitati sia gli accessi POP che IMAP.

Account disabilitato. È disabilitato qualsiasi accesso all'account.

Account di sistema. Account di sistema di MDaemon.

Mostra solo gli account di questo dominio
Per visualizzare tutti gli account di MDaemon, selezionare "Tutti i domini" nella casella di riepilogo a discesa. Per visualizzare solo gli account di un dominio, selezionare il dominio desiderato.

Nuovo
Per creare un nuovo account, fare clic su questo pulsante e aprire Account Editor 343.

Modifica
Selezionare un account nell'elenco, quindi fare clic su questo pulsante per aprirlo in Account Editor 343.

Elimina
Per eliminare un account, selezionarlo e fare clic su questo pulsante. Verrà chiesto di confermare l'operazione.

Mostra più account
L'elenco visualizza solo 500 account alla volta. Se il dominio selezionato contiene più

di 500 account, fare clic su questo pulsante per visualizzare i 500 account successivi. Vedere la nota precedente per istruzioni su come incrementare il numero massimo di account visualizzabili.

Superiore
Fare clic su questo pulsante per spostarsi rapidamente all'inizio dell'elenco.

Importa
Fare clic su questo pulsante per importare gli account da un file di testo delimitato da virgole. Con questo pulsante si ottiene lo stesso risultato che si otterrebbe con la selezione di menu Account » Importazione » Importa account da file di testo delimitato da virgole.

Valori predefiniti
Questo pulsante consente di aprire la finestra di dialogo Valori predefiniti nuovo account 377.

Rimuovi da elenco
Selezionare uno o più account, quindi fare clic su questo pulsante per annullarne le iscrizioni dalle Liste di distribuzione 431 ospitate sul server. Viene aperta una finestra che chiede di confermare la rimozione degli indirizzi dalle liste.

Per ulteriori informazioni, vedere:

Valori predefiniti nuovo account 377
Account Editor 343

6.1.1 Account Editor

6.1.1.1 Dettagli account

Account

Attiva questo account
Per disabilitare tutti gli accessi all'account, deselezionare questa casella di controllo. L'utente non sarà in grado in alcun modo di accedere all'account e MDaemon non ne accetterà la posta. L'account non verrà eliminato e verrà utilizzato per calcolare il numero di licenze utilizzate, ma MDaemon si comporterà come se l'account non esistesse.

Nome e cognome
Inserire in questo campo il nome e il cognome dell'utente. Quando si crea un nuovo account, molti dei campi delle varie schermate di Account Editor vengono compilati automaticamente al momento dell'inserimento del nome e del cognome dell'utente. Le informazioni generate automaticamente si basano sui modelli e sulle impostazioni di Valori predefiniti nuovo account 377. Il campo relativo al nome e al cognome non può contenere caratteri "!" o "|".

Indirizzo e-mail
Questo campo consente di specificare l'indirizzo e-mail dell'account. Quando si crea un nuovo account, la parte dell'indirizzo relativa alla casella postale viene compilata automaticamente al momento dell'inserimento di *Nome e cognome*, in base al modello di *casella postale* indicato in: Valori predefiniti nuovo account » Casella postale 377. Se non si desidera utilizzare quello generato automaticamente, è possibile inserire manualmente un nome diverso per la casella postale. Quindi, fare

clic sulla casella di riepilogo a discesa dopo il simbolo "@" per prelevare il dominio di appartenenza dell'account. Per impostazione predefinita, nell'elenco a discesa viene visualizzato il dominio predefinito 41 di MDaemon. L'indirizzo e-mail completo viene utilizzato come identificativo univoco dell'account e come ID utente per POP3, IMAP, WorldClient e così via. Gli indirizzi e-mail non possono contenere caratteri di spaziatura, "!" o "|".

Password e-mail
È la password utilizzata dall'account per l'invio e la ricezione di posta POP3 o IMAP con MDaemon, per l'autenticazione durante il processo SMTP oppure per la connessione mediante WorldClient, WebAdmin o Outlook Connector. Al di sotto di quest'area viene visualizzata una breve frase che indica se l'account utilizza l' autenticazione dinamica 422.

È necessario fornire sempre la *password e-mail*, anche se non si desidera consentire l'accesso POP3/IMAP all'account di posta. Oltre che per la verifica della sessione di posta, i valori *Indirizzo e-mail* e *Password e-mail* vengono utilizzati per consentire la modifica remota dell'account e il recupero remoto dei file. Se si desidera impedire l'accesso POP/IMAP, utilizzare le opzioni *L'account utilizza [POP3/MultiPOP/IMAP/OC (Outlook Connector)]*. Se si desidera impedire tutte le modalità di accesso, deselezionare l'opzione *Attiva questo account*.

L'account utilizza

POP3
Se non si desidera che l'utente possa accedere al proprio account mediante POP3, deselezionare questa casella di controllo. L'account sarà ancora accessibile tramite IMAP, WorldClient o WebAdmin, se queste opzioni sono abilitate.

MultiPOP
Selezionare questa casella di controllo se si desidera che l'account utilizzi MultiPOP 367.

IMAP
Se non si desidera che l'utente acceda al proprio account tramite IMAP, deselezionare questa casella di controllo. L'account sarà ancora accessibile tramite POP3, WorldClient o WebAdmin, se queste opzioni sono abilitate.

OC (ossia Outlook Connector)
Scegliere questa opzione se si desidera che l'account condivida le cartelle di Microsoft Outlook mediante Outlook Connector per MDaemon 405. **Nota:** questa opzione è disponibile solo se è installato Outlook Connector.

Password SyncML
Questa opzione consente di specificare una password differente per l'account, da utilizzare per l'interazione con il server SyncML 135. Se non viene specificato alcun valore, per le connessioni SyncML viene utilizzata la *password e-mail* dell'account.

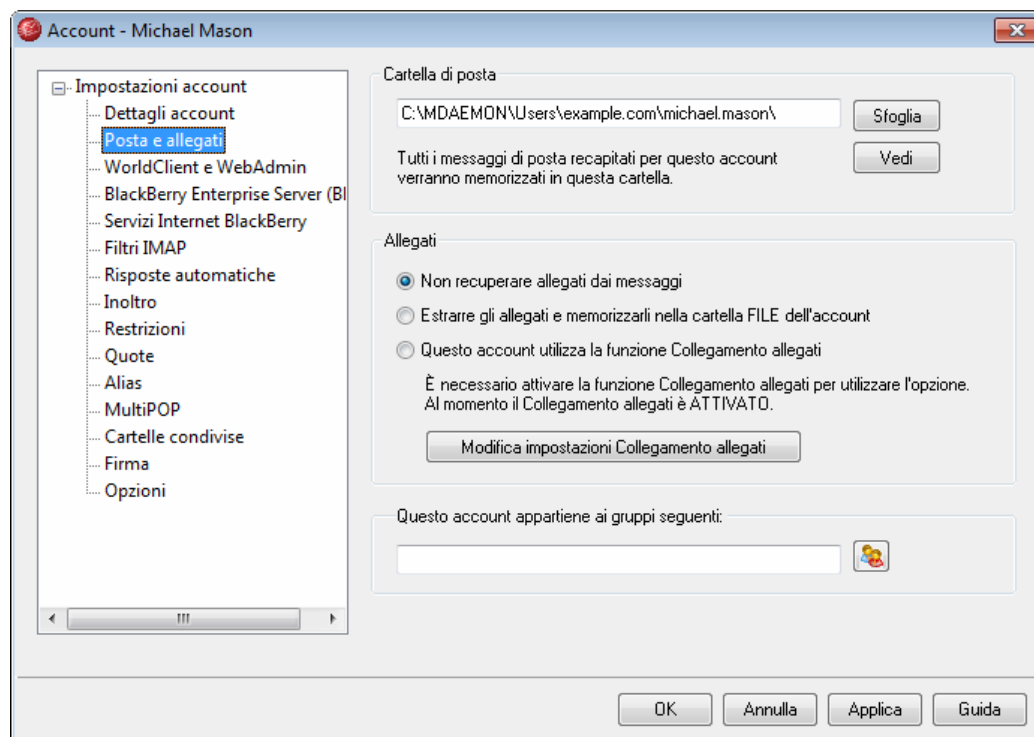
Per gli account che utilizzano l'autenticazione dinamica, tuttavia, la password SyncML è obbligatoria perché non è possibile accedere al server SyncML con tale metodo di autenticazione.

Utente/password host intelligente

Se è abilitata l'opzione *Consenti autenticazione in base ad account* della schermata Consegna 42 situata in Impostazioni » Dominio predefinito/servere per questo account si desidera utilizzare l'autenticazione in base all'account anziché le credenziali indicate nella schermata, è necessario specificare le credenziali facoltative dell'account per l'host intelligente. Se non si desidera utilizzare l'autenticazione in base all'account, lasciare il campo vuoto.

Note/commenti sull'account

Utilizzare quest'area di testo per immettere eventuali note o commenti sull'account.

6.1.1.2 Posta e allegati

Cartella di posta

Immettere il nome della cartella nella quale si desidera memorizzare i messaggi e-mail relativi all'account. La posizione predefinita della cartella in fase di creazione di un nuovo account è basata sul campo *Modello cartella posta* indicato in: Valori predefiniti nuovo account » Casella 377.

Allegati

Non recuperare allegati dai messaggi
Con questa opzione, gli allegati non vengono estratti dai messaggi dell'account. I messaggi con allegati vengono gestiti normalmente e gli allegati rimangono invariati.

Estrarre gli allegati e memorizzarli nella cartella FILE dell'account
Se impostata, questa opzione indica a MDaemon di estrarre automaticamente tutti gli eventuali file incorporati MIME Base64 allegati ai messaggi di posta in arrivo dell'account. I file estratti vengono rimossi dal messaggio in arrivo, decodificati e collocati nella sottocartella `\Files\`. Quindi, nel corpo del messaggio viene inserita una nota, con l'elenco dei nomi dei file estratti. Questa opzione non offre un collegamento agli allegati memorizzati, pertanto per recuperarli è necessario disporre dei diritti di accesso alla rete appropriati.

Gli account utilizzano la funzione Collegamento allegati
Con questa opzione gli allegati vengono estratti dai messaggi in arrivo dell'account e memorizzati nella posizione indicata nella finestra di dialogo Collegamento allegati 154. I collegamenti URL vengono quindi inseriti nel corpo del messaggio, dove è possibile selezionarli per scaricare i file. Per motivi di sicurezza, i collegamenti URL non contengono i percorsi diretti ai file. Contengono invece un identificativo univoco (GUID) utilizzato dal server per mappare il file al percorso effettivo. La mappatura dei GUID è memorizzata nel file `AttachmentLinking.dat`.

Se questa opzione è selezionata, ma la funzione Collegamento allegati della finestra di dialogo Collegamento allegati 154 è disabilitata, gli allegati non vengono estratti.

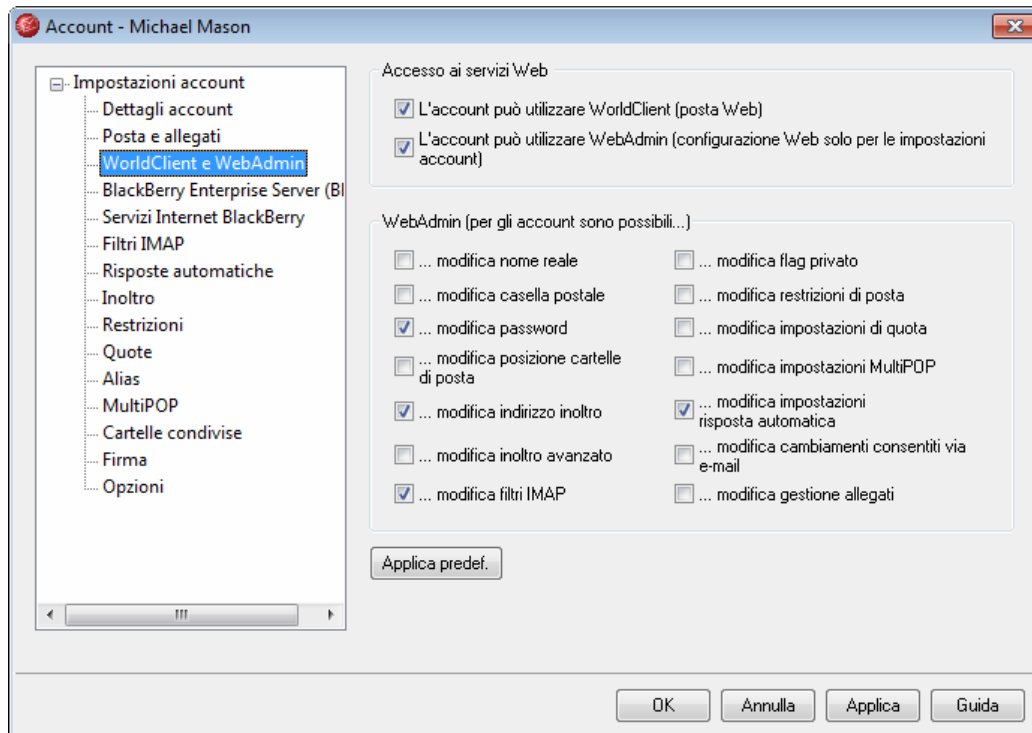
Modifica impostazioni Collegamento allegati
Questo pulsante consente di aprire la finestra di dialogo Collegamento allegati 154.

Gruppi

Questo account appartiene ai gruppi seguenti:
Questa casella consente di aggiungere l'account a uno o più gruppi 417. Separare ogni gruppo con uno spazio o utilizzare l'icona Account per esplorare la lista dei gruppi disponibili.

Vedere:

Collegamento allegati 345
Valori predefiniti nuovo account » Casella postale 377
Gruppi 417

6.1.1.3 WorldClient e WebAdmin

Accesso ai servizi Web

L'account può utilizzare WorldClient (posta Web)
Selezionare questa casella di controllo se si desidera autorizzare l'account ad accedere al server WorldClient 117, che consente di controllare i messaggi di e-mail mediante un browser Web.

L'account può utilizzare WebAdmin (configurazione Web solo per le impostazioni account)
Abilitare questa casella per autorizzare gli utenti alla modifica delle impostazioni dell'account mediante WebAdmin 144. Gli utenti potranno modificare solo le impostazioni specificate successivamente.

Se si abilita questa funzione e se il server WebAdmin è attivo, è possibile accedere a WebAdmin inserendo nel browser il dominio di MDaemon desiderato e la porta assegnata a WebAdmin 145 (ad esempio, `http://esempio.com:1000`). Dapprima viene visualizzata una schermata di registrazione, quindi la schermata delle impostazioni che si è autorizzati a modificare. È sufficiente modificare le impostazioni desiderate e fare clic sul pulsante *Salva modifiche*. Quindi, uscire e chiudere il browser. Se si dispone dell'accesso a WorldClient è possibile accedere a WebAdmin anche dal menu Opzioni avanzate di WorldClient.

Se l'utente è un amministratore globale o un amministratore di dominio, privilegio indicato nella schermata Opzioni 374 di Account Editor, dopo l'accesso a WebAdmin verrà visualizzata una schermata diversa.

WebAdmin (per gli account sono possibili)

...modifica nome reale
Abilitando questa funzione, l'utente può modificare l'impostazione *Nome e cognome*.

...modifica casella postale
Abilitando questa funzione, l'utente può modificare la parte dell'*indirizzo e-mail* relativa alla propria casella postale.

Poiché il nome della casella postale fa parte dell'indirizzo e-mail dell'account e rappresenta l'identificativo univoco e il valore dell'ID utente utilizzato per l'accesso, modificarla significa modificare l'effettivo indirizzo e-mail dell'utente. Ciò può determinare il rifiuto, l'eliminazione o comunque la perdita dei futuri messaggi diretti al precedente indirizzo.

...modifica password
Selezionare questa casella di controllo per consentire all'utente di modificare la *password e-mail dell'account.*

...modifica posizione cartelle di posta
Abilitando questa casella, l'utente viene autorizzato a modificare la cartella dei messaggi 345 dell'account.

È opportuno prestare particolare cautela nel concedere questa autorizzazione. Infatti, la modifica della cartella dei messaggi consente di influire su tutte le cartelle del server.

...modifica indirizzo inoltro
Quando questa funzione è abilitata, l'utente è in grado di modificare le impostazioni dell'indirizzo di inoltro 360.

...modifica inoltro avanzato
Quando questa funzione è abilitata, l'utente è in grado di modificare le *opzioni di inoltro avanzate.*

...modifica filtri IMAP
Questa opzione consente all'utente di creare e gestire i propri filtri di posta 353. Questa funzione è disponibile solo in MDaemon PRO.

...modifica flag privato
Questa opzione indica se l'utente può utilizzare WebAdmin per modificare l'opzione "*Account privato*" della schermata Opzioni 374 di Account Editor.

...modifica restrizioni di posta
Questa casella di controllo consente di autorizzare l'account alla modifica delle limitazioni relative alla posta in entrata e in uscita, situate nella schermata

Restrizioni 361.

...modifica impostazioni di quota
Con questa casella di controllo è possibile consentire all'account la modifica delle impostazioni relative alla quota 364.

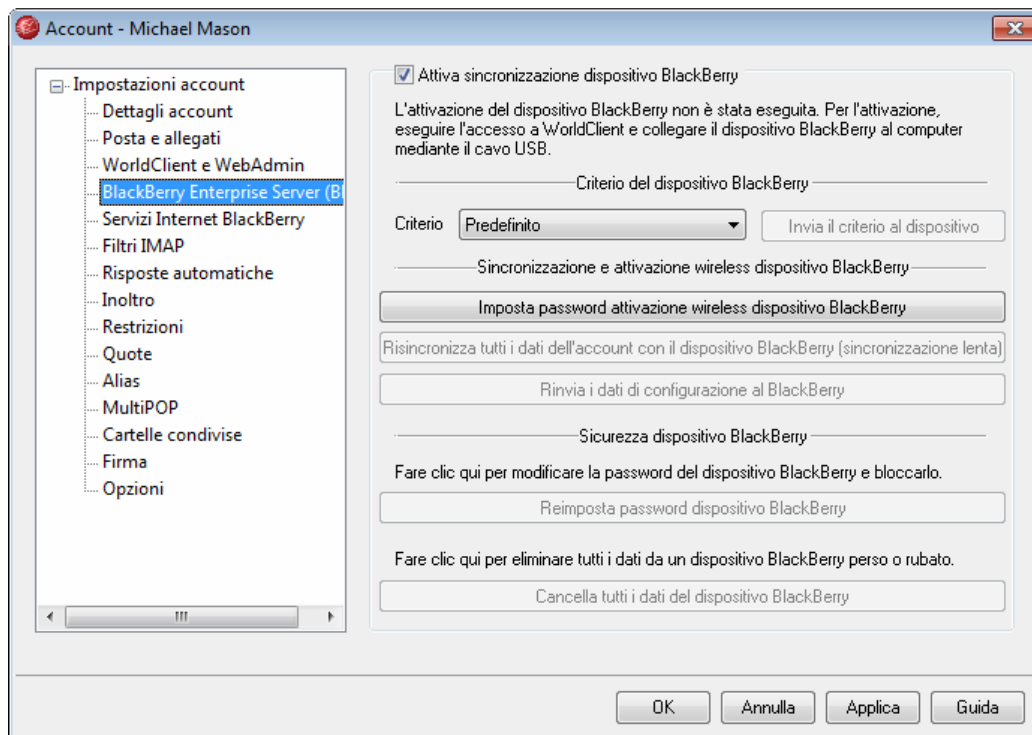
...modifica impostazioni MultiPOP
Selezionare questa casella di controllo per consentire all'account di aggiungere nuove voci MultiPOP 367 e di attivare/disattivare la raccolta di posta MultiPOP per tali voci.

...modifica impostazioni risposta automatica
Selezionare questa casella di controllo per consentire all'utente di aggiungere, modificare o eliminare le risposte automatiche 357 per il proprio account.

...modifica cambiamenti consentiti via e-mail
Selezionare questa casella di controllo per consentire agli utenti di modificare le *impostazioni dell'account* mediante messaggi e-mail con formattazione speciale 506.

...modifica gestione allegati
Se si seleziona questa casella, l'utente ha la possibilità di modificare le opzioni di gestione degli allegati dell'account nella schermata Posta e allegati 345.

Applica predefiniti
Questo pulsante consente di riportare le impostazioni della schermata ai valori predefiniti indicati nella schermata WorldClient e WebAdmin 382, disponibile in: Account » Impostazioni account » Valori predefiniti nuovo account.

6.1.1.4 BES BlackBerry

Le opzioni di questa schermata determinano le impostazioni BES di un dato account e consentono di effettuare diverse operazioni relative al dispositivo BlackBerry per l'account attivato.

Abilita questo account all'uso di BlackBerry

Selezionare questa casella di controllo per abilitare l'account all'utilizzo di BlackBerry. Gli account abilitati per BlackBerry vengono visualizzati nella schermata BES BlackBerry » Account integrati 177 e possono attivare un dispositivo BlackBerry tramite cavo USB in WorldClient o via radio (OTA) dal dispositivo stesso, sebbene non tutti i dispositivi supportino l'attivazione OTA.

Dopo l'attivazione di un dispositivo, in questa sezione ne vengono elencati il PIN, la versione della piattaforma, il modello e il numero di telefono.

Dopo aver abilitato un account per BlackBerry, il database BES inizia a memorizzare informazioni sui messaggi e sui dati dell'account in modo da sincronizzarlo 181 con il dispositivo BlackBerry al momento della sua attivazione. Tutti i messaggi elaborati per l'account da quando questo è stato abilitato per BlackBerry vengono sincronizzati con il dispositivo al momento della sua attivazione.

Se si deseleziona questa opzione, vengono eliminati tutti i dati BES relativi all'account. Se si abilita nuovamente l'account per BlackBerry, la memorizzazione dei dati riprenderà e sarà

necessario riattivare il dispositivo.

Criterio del dispositivo BlackBerry

Criterio
Selezionare nell'elenco a discesa il criterio 170 che verrà utilizzato dal dispositivo dopo l'attivazione.

Invia il criterio al dispositivo
Nel caso si desideri inviare un nuovo criterio a un dispositivo già attivato, selezionare il criterio nell'elenco a discesa e fare clic su questo pulsante.

Sincronizzazione e attivazione wireless dispositivo BlackBerry

Imposta password di attivazione aziendale wireless
Per impostare una password Attivazione azienda wireless per l'account, fare clic su questo pulsante, immettere la password e fare clic su **OK**. L'utente può quindi immettere l'indirizzo di posta elettronica dell'account e la password di Attivazione azienda nella schermata Attivazione azienda del dispositivo per attivarlo via radio (OTA). Non tutti i dispositivi possono essere attivati in modalità wireless.

Risincronizza tutti i dati dell'account con il dispositivo BlackBerry (sincronizzazione lenta)
Per risincronizzare tutti i dati dell'account con il dispositivo, nella finestra di dialogo di conferma fare clic su questo pulsante e quindi su **OK**. Questa operazione è comunemente denominata "sincronizzazione lenta" e garantisce la coerenza dei dati del dispositivo BlackBerry con quelli di MDaemon. In base all'entità dei dati, tale operazione potrebbe richiedere diversi minuti. Dopo l'avvio, l'operazione di sincronizzazione lenta viene eseguita in background fino al completamento. Nella schermata BlackBerry BES » Account integrati 177 è disponibile un'opzione che consente di risincronizzare **tutti** i dispositivi BlackBerry attivati. Per ulteriori informazioni sulle opzioni di sincronizzazione BES, consultare BlackBerry BES » Opzioni 180.

Rinvia i dati di configurazione al BlackBerry
Per inviare nuovamente i libri di servizio al dispositivo BlackBerry dell'account, fare clic su questo pulsante e quindi su **Sì** nella finestra di dialogo di conferma.

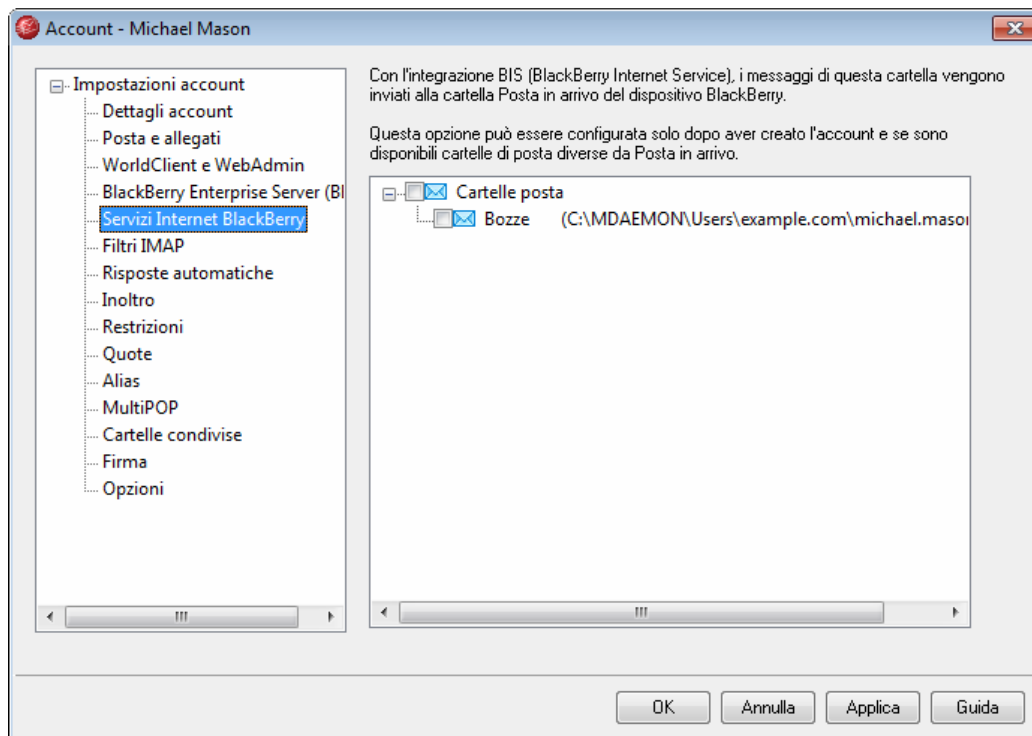
Sicurezza dispositivo BlackBerry

Reimposta password dispositivo BlackBerry
Per reimpostare la password del dispositivo in modalità remota, fare clic su questo pulsante, immettere la password e fare clic su **OK**.

Cancella tutti i dati del dispositivo BlackBerry
Per cancellare tutti i dati del dispositivo BlackBerry in modalità remota, ad esempio in caso di smarrimento o di furto, fare clic su questo pulsante e, quindi, su **Sì** nella finestra di dialogo di conferma.

Vedere:

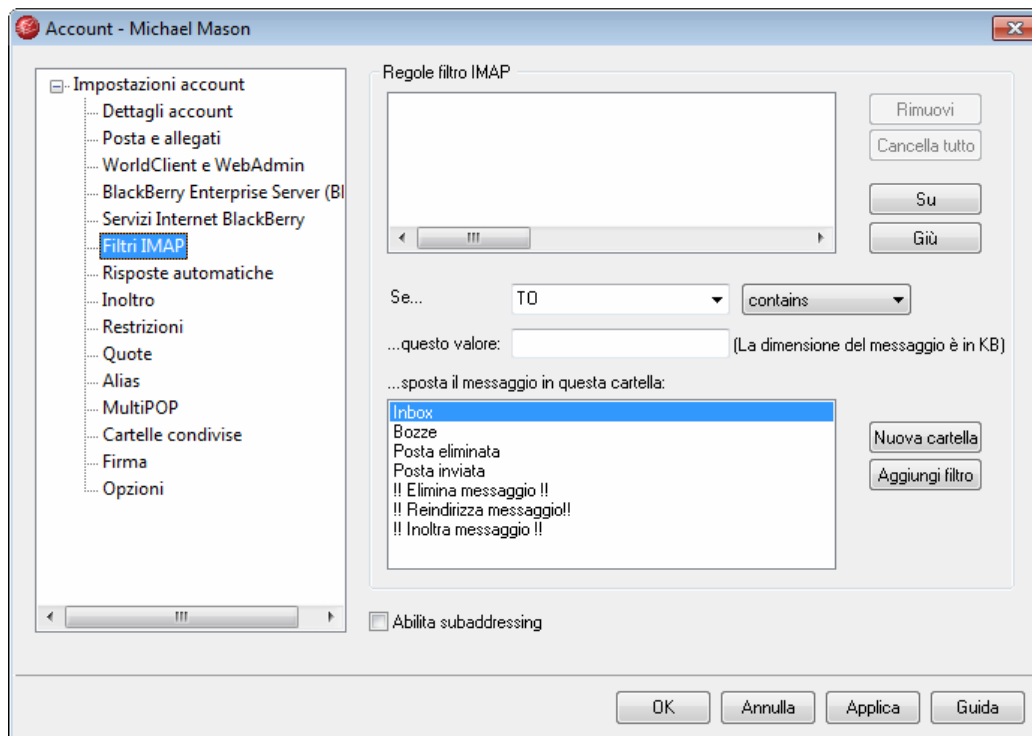
[BES BlackBerry](165)

6.1.1.5 BIS BlackBerry

Se per raccogliere la posta elettronica dell'account con uno smartphone BlackBerry si utilizzano i Servizi Internet BlackBerry (BIS, BlackBerry Internet Service), in questa schermata è possibile specificare le cartelle IMAP i cui nuovi messaggi devono essere inviati alla Posta in arrivo dello smartphone. Generalmente i servizi Internet BlackBerry raccolgono solo i messaggi della cartella Posta in arrivo dell'utente, ignorando i messaggi nelle altre cartelle associate all'account dell'utente. Pertanto i messaggi ordinati automaticamente mediante i filtri IMAP[353] in particolari cartelle non vengono consegnati al dispositivo BlackBerry. Questa schermata consente di ricevere i messaggi filtrati da qualsiasi cartella si desideri. Non consente tuttavia di ricevere i messaggi già contenuti nelle cartelle, ma solo i nuovi messaggi. Se l'account è privo di filtri IMAP, questa schermata rimane vuota.

Al dispositivo BlackBerry non viene inviato il contenuto dell'intera cartella, ma solo i nuovi messaggi. I messaggi vengono consegnati alla Posta in arrivo del dispositivo e non ad altre cartelle specifiche.

Per gli utenti che hanno accesso a WorldClient, questa opzione si trova nella pagina Cartelle di Opzioni, pertanto gli utenti possono gestire autonomamente la selezione della cartella. Questa opzione, tuttavia, è disponibile solo se è stata abilitata l'opzione "*Consenti selezione contenuto di cartelle diverse da Posta in entrata per l'invio a BlackBerry*" della schermata BlackBerry BIS Options 190.

Vedere:

6.1.1.6 Filtri IMAP

MDaemon consente agli utenti IMAP e WorldClient 117 di smistare automaticamente la posta in specifiche cartelle sul server mediante filtri. Analogamente ai filtri di contenuto 212, le intestazioni di ciascun messaggio in entrata dell'account vengono esaminate e confrontate con i filtri definiti per l'account. Quando un messaggio indirizzato al titolare dell'account corrisponde a uno dei filtri, MDaemon lo sposta nella cartella specificata dal filtro in questione. Questo metodo è molto più efficace, sia per il client sia per il server, rispetto al filtro dei messaggi del client e, poiché alcuni client di posta non supportano le regole o il filtro dei messaggi locali, consente di sopperire a tale mancanza.

Gli amministratori possono creare i filtri mediante la schermata Filtri IMAP di Account Editor o utilizzando WebAdmin 144. È tuttavia possibile offrire agli utenti l'autorizzazione per la creazione e la gestione autonoma dei filtri mediante WorldClient o WebAdmin. Tali autorizzazioni possono essere impostate nella schermata WorldClient e WebAdmin 347.

Regole di filtro IMAP

In questa casella viene visualizzato l'elenco di tutti i filtri creati per l'account

dell'utente. I filtri vengono elaborati nell'ordine in cui sono elencati fino al rilevamento di una corrispondenza. Di conseguenza, quando un messaggio corrisponde a uno dei filtri, viene spostato nella cartella specificata nel filtro stesso e l'elaborazione dei filtri per tale messaggio viene terminata. Utilizzare i pulsanti *Su* e *Giù* per spostare i filtri all'interno dell'elenco.

Rimuovi
Selezionare un filtro, quindi fare clic su *Rimuovi* per eliminarlo dall'elenco.

Cancella tutto
Fare clic su questo pulsante per eliminare tutti i filtri dell'utente.

Su
Selezionare un filtro, quindi scegliere questo pulsante per spostarlo più in alto all'interno dell'elenco.

Giù
Selezionare un filtro, quindi scegliere questo pulsante per spostarlo più in basso all'interno dell'elenco.

Se [intestazione messaggio/dimensione messaggio]
Selezionare "*MESSAGE SIZE (Dimensione messaggio)*" o un'intestazione in questa casella di riepilogo a discesa oppure digitare l'intestazione desiderata qualora non sia presente. Se si indica un'intestazione, MDaemon cerca il testo della casella "*questo valore*" nelle intestazioni corrispondenti di tutti i messaggi in entrata relativi all'account. Quindi, in base al tipo di confronto in corso, determina quali messaggi spostare nella cartella specificata nel filtro.

Tipo di confronto
In questo elenco a discesa è possibile scegliere il tipo di confronto relativo all'intestazione o alla dimensione del messaggio indicata nel filtro. MDaemon cerca nell'intestazione specificata il testo contenuto nel campo "*questo valore*" (oppure confronta la dimensione del messaggio con tale valore) ed esegue il confronto in base all'impostazione di questa opzione, ad esempio verifica se il testo completo dell'intestazione corrisponde esattamente, non corrisponde esattamente, contiene il testo, non lo contiene e così via.

...questo valore
Immettere il testo da cercare durante la scansione dell'intestazione di messaggio specificata per il filtro. Se l'impostazione del filtro prevede il controllo della dimensione del messaggio, specificare i KB.

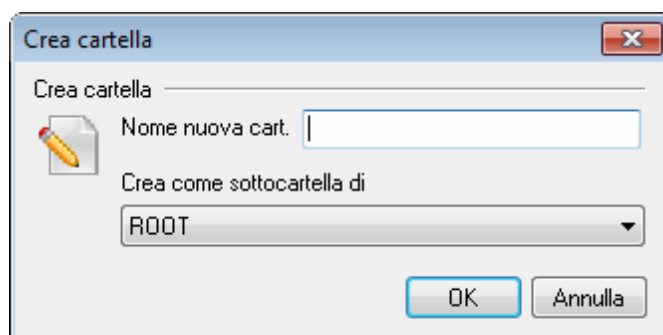
...sposta il messaggio in questa cartella
Una volta specificati i parametri per il filtro, selezionare la cartella in cui si desidera spostare i messaggi che corrispondono al filtro, quindi fare clic sul pulsante *Aggiungi filtro* per creare il filtro desiderato. L'elenco include anche tre voci speciali: "*!!Elimina messaggio!!*," "*!!Reindirizza messaggio!!*" e "*!!Inoltra messaggio!!*."

!! Elimina messaggio !! - Dopo aver scelto i valori dei filtri e aver selezionato questa opzione, facendo clic su *Aggiungi filtro* verrà creato un filtro che determinerà l'eliminazione del messaggio quando quest'ultimo corrisponde alle

condizioni previste.

!! Reindirizza messaggio!! - Dopo aver scelto i valori dei filtri e aver selezionato questa opzione, fare clic su *Aggiungi filtro* e inserire un indirizzo e-mail. In tal modo verrà creato un filtro che determinerà il reindirizzamento del messaggio all'indirizzo e-mail specificato. Le intestazioni e il corpo del messaggio non vengono modificati. Le uniche modifiche apportate interessano il destinatario della busta SMTP.

!! Inoltra messaggio !! - Dopo aver scelto i valori dei filtri e aver selezionato questa opzione, fare clic su *Aggiungi filtro* e inserire un indirizzo e-mail. In tal modo verrà creato un filtro che determinerà l'inoltro del messaggio all'indirizzo e-mail specificato. Viene creato e inviato un nuovo messaggio con l'intestazione Subject e il contenuto del messaggio originale.

Nuova cartella
Fare clic su questo pulsante per creare una nuova cartella. Verrà aperta la finestra di dialogo per la creazione delle cartelle, in cui è possibile assegnare un nome alla cartella. Se si desidera creare una sottocartella di una cartella esistente, scegliere quest'ultima dall'elenco a discesa.

Aggiungi Filtro
Dopo aver concluso la definizione delle condizioni relative al filtro, fare clic su questo pulsante per aggiungerlo all'elenco.

Subaddressing

Il subaddressing è una tecnica che consente di includere il nome di una cartella nella parte relativa alla casella postale di un indirizzo e-mail. Utilizzando questa tecnica, i messaggi destinati alla combinazione *casella postale+nome cartella* vengono instradati automaticamente alla cartella dell'account inclusa nell'indirizzo, senza che sia necessario creare regole di filtro a tale scopo.

Se, ad esempio, `franco.tommaso@esempio.com` ha una cartella di posta IMAP denominata "`materiale`," la posta in arrivo all'indirizzo "`franco.tommaso+materiale@esempio.com`" verrà instradata automaticamente in tale cartella. Per specificare sottocartelle è possibile separare i nomi della cartella e della sottocartella con un carattere aggiuntivo "+", mentre per sostituire eventuali spazi presenti nei nomi delle cartelle è necessario utilizzare il carattere di sottolineatura. Utilizzando l'esempio precedente, se nella cartella "`materiale`" di Franco è presente una sottocartella denominata "`materiale vecchio`," i messaggi inviati a "`franco.`

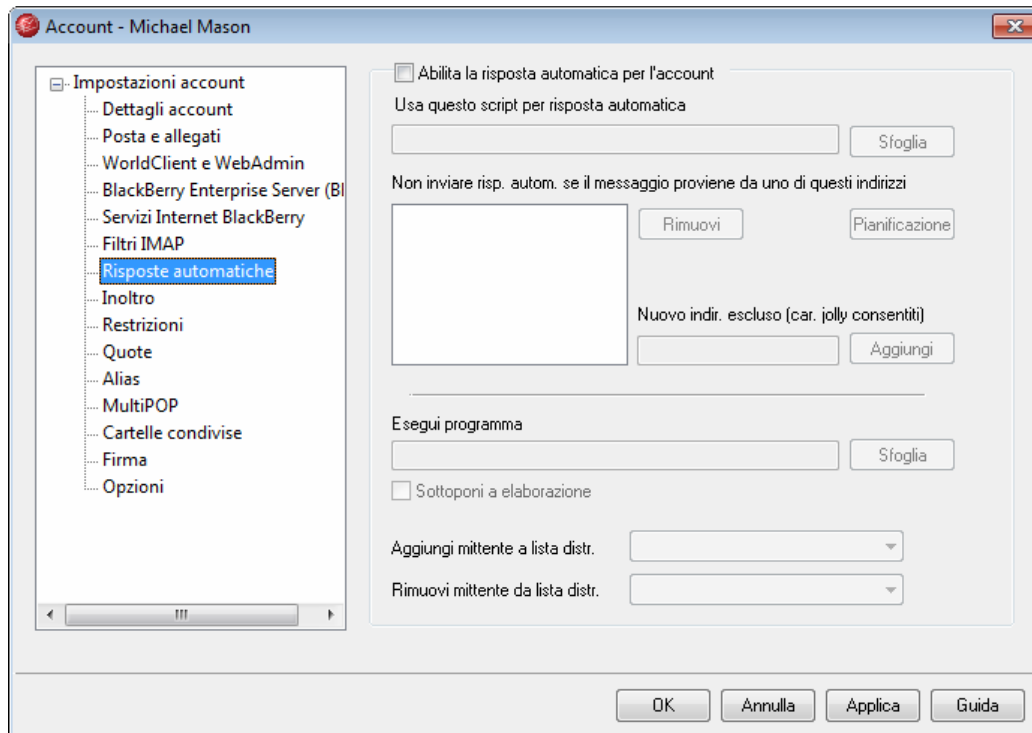
tommaso+materiale.materiale_vecchio@esempio.com" verranno instradati automaticamente alla cartella di posta "\materiale\materiale vecchio\" di Franco.

Poiché il subaddressing prevede l'utilizzo del carattere "+", non è possibile utilizzare questa tecnica con le caselle postali il cui nome contiene "+". Nell'esempio precedente, se l'indirizzo effettivo fosse "franco+tommaso@esempio.com", anziché "franco.tommaso@esempio.com", la funzionalità di subaddressing non potrebbe essere utilizzata. Inoltre, non è possibile utilizzare un alias di indirizzo con questa tecnica. È possibile, tuttavia, creare un alias che fa riferimento all'intero indirizzo con subaddressing. Di conseguenza, anche se "alias+materiale@esempio.com" non è consentito, è possibile utilizzare "alias@esempio.com" per indicare "franco.tommaso+materiale@esempio.com".

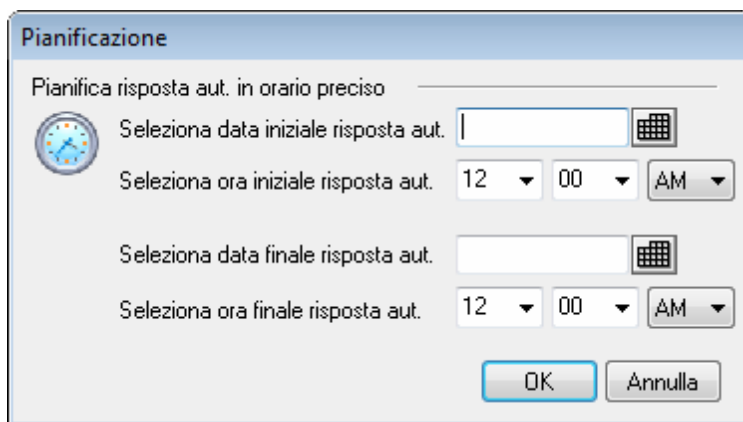
Per impedire l'uso improprio o fraudolento di questa funzionalità, la cartella IMAP inclusa nell'indirizzo con subaddressing **deve** essere valida. Se il subaddressing di un messaggio in arrivo fa riferimento a una cartella non esistente per l'account, l'indirizzo viene considerato come indirizzo di posta non esistente e gestito in base alle relative impostazioni definite in MDaemon. Se, ad esempio, per franco@esempio.com non esiste una cartella denominata "materiale" e si riceve un messaggio indirizzato a "franco+materiale@esempio.com", il messaggio viene considerato come indirizzato a un utente sconosciuto e, molto probabilmente, respinto.

Abilita subaddressing
Selezionare questa casella di controllo se si desidera consentire il subaddressing per l'account.

Per impostazione predefinita, il subaddressing è disabilitato per tutti gli account. È possibile disattivare questa funzionalità a livello globale mediante l'opzione *Disabilita funzione subaddressing per tutti gli account* della schermata Varie 202 presente nella finestra di dialogo Preferenze. In questo caso, tale funzionalità viene disattivata per tutti gli account, indipendentemente dalle impostazioni dei singoli account.

6.1.1.7 Risposte automatiche

Le risposte automatiche sono strumenti che consentono, in base ai messaggi in entrata, di attivare eventi specifici quali l'esecuzione di un programma, l'inserimento di un mittente in una lista di distribuzione, l'invio di una risposta con un messaggio generato automaticamente e altro ancora. L'utilizzo più comune delle risposte automatiche consiste nella risposta automatica ai messaggi in entrata con un messaggio definito dall'utente con il quale viene comunicato che l'utente è in vacanza, non è disponibile, risponderà appena possibile e così via. Gli utenti di MDaemon che utilizzano l'accesso Web 347 con WorldClient 117 o con WebAdmin 144 possono utilizzare le opzioni disponibili per comporre i propri messaggi di risposta automatica e pianificarne le date. I messaggi di risposta automatica si basano su script di risposta, ossia file con estensione `*.RSP`, nei quali è possibile utilizzare numerose macro. Tali macro consentono la generazione dinamica di gran parte del contenuto degli script, rendendo le risposte automatiche particolarmente versatili.

Gli eventi di risposta automatica vengono utilizzati quando il messaggio di attivazione proviene da un'origine remota. Per i messaggi con origine locale, tuttavia, le risposte automatiche vengono attivate solo se è abilitata l'opzione *Risposte automatiche attivate da posta interna al dominio* della schermata Risposte automatiche » Opzioni 389. Questa schermata consente inoltre di utilizzare un'opzione per limitare i messaggi di risposta automatica a una risposta al giorno per ogni mittente.

Abilita la risposta automatica per l'account
Selezionare questa casella di controllo per attivare una risposta automatica per l'account. Per ulteriori informazioni sulle risposte automatiche, consultare: Risposte automatiche 387.

Usa questo script per riposta automatica
In questo campo è possibile specificare il percorso e il nome del file di risposta (`*.RSP`), elaborato e utilizzato per comporre il messaggio da restituire al mittente. Gli script di risposta possono contenere macro da utilizzare per rendere dinamici i messaggi di risposta e per automatizzarne gran parte del contenuto. Per ulteriori informazioni, vedere Creazione degli script di risposta automatica 390.

Pianificazione
Fare clic su questo pulsante per aprire la finestra di dialogo Pianificazione, che consente di impostare la data e l'ora di inizio e di fine dell'intervallo temporale in cui deve essere attiva la funzione di risposta automatica. Se si desidera che la risposta automatica sia sempre attiva, lasciare i campi vuoti.

Non inviare risp. autom. se il messaggio proviene da uno di questi indirizzi
In questo campo è possibile elencare gli indirizzi che si desidera escludere dall'invio della risposta automatica.

Può accadere che i messaggi di risposta automatica vengano inviati a un indirizzo che utilizza a sua volta lo stesso meccanismo. In questo caso, viene a crearsi un effetto "ping-pong" per cui i messaggi vengono continuamente scambiati tra i due server. Per evitare tale problema è possibile inserire l'indirizzo in questo campo. Nella schermata Risposte automatiche » Opzioni 389 è disponibile un'opzione che consente di limitare i messaggi di risposta automatica a non più di uno al giorno per ogni mittente.

Rimuovi
Fare clic su questo pulsante per eliminare le voci selezionate dall'elenco degli indirizzi esclusi.

Nuovo indir. escluso (car. jolly consentiti)
Se si desidera aggiungere un indirizzo all'elenco degli indirizzi esclusi, inserirlo in questo campo e fare clic sul pulsante *Aggiungi*.

Esecuzione di un programma

Esegui programma
Questo campo consente di specificare il percorso e il nome del file in un programma da eseguire all'arrivo della posta in questo account. Accertarsi che tale programma termini in modo corretto e possa essere eseguito senza supervisione. È possibile inserire eventuali parametri della riga di comando subito dopo il percorso del file eseguibile.

Sottoponi a elaborazione
Se si seleziona questa opzione, il nome del messaggio di attivazione verrà passato al processo specificato nel campo *Esegui questo programma* come primo parametro disponibile della riga di comando. Se si imposta la risposta automatica per un account che inoltra la posta a un'altra posizione **senza** conservarne copia locale nella propria casella postale (vedere inoltro 360), questa funzione viene disabilitata.

Per impostazione predefinita, MDaemon inserisce il nome del file di messaggio come ultimo parametro della riga di comando. Per ignorare questa funzione, utilizzare la macro `$MESSAGE$`. Inserire la macro al posto del nome file del messaggio. Ciò consente di aumentare la flessibilità della funzione, in quanto sarà possibile utilizzare righe di comando complesse come la seguente: `logmail /e /j /message=$MESSAGE$ /q`.

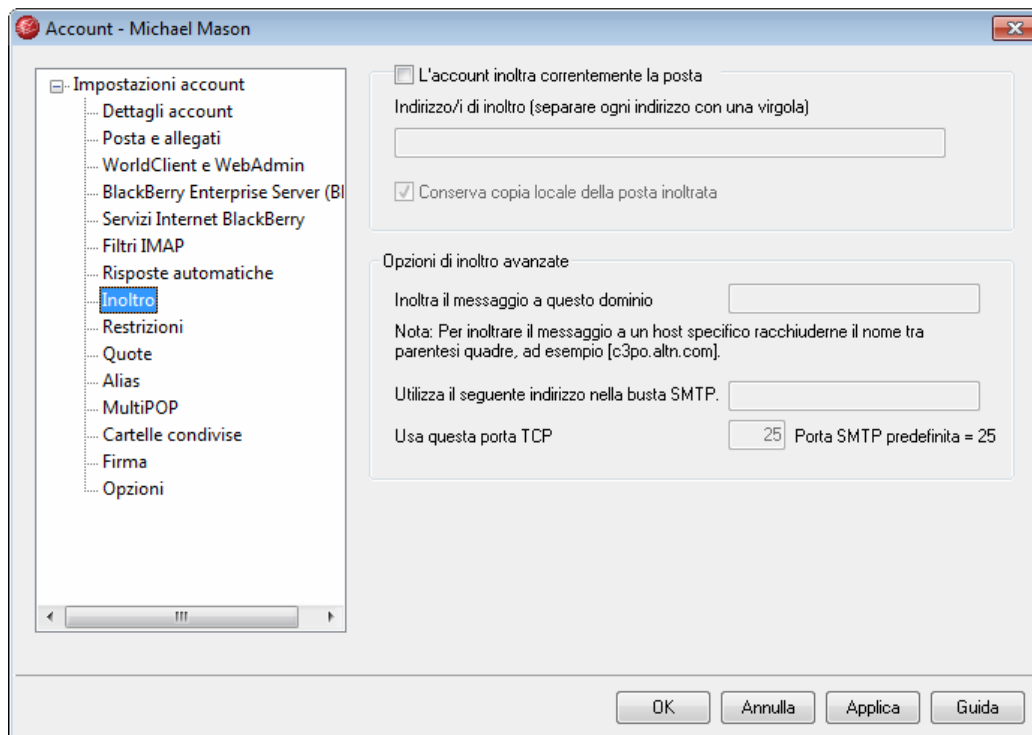
Liste di distribuzione

Aggiungi mittente a lista distr.
Se in questo campo si specifica una lista di distribuzione, il mittente del messaggio in entrata diventa automaticamente un membro di tale lista. Questa funzione è molto utile per la creazione automatica delle liste.

Rimuovi mittente da lista distr.
Se in questo campo si specifica una lista di distribuzione, il mittente del messaggio in entrata viene rimosso automaticamente dalla lista indicata.

Vedere:

Risposte automatiche » Account 387
Risposte automatiche » Lista bianca 388
Risposte automatiche » Opzioni 389
Creazione degli script di risposta automatica 390

6.1.1.8 Inoltro

Opzioni di inoltro posta

L'account inoltra correntemente la posta
Se si abilita questa casella, i messaggi in entrata dell'account vengono inoltrati agli indirizzi indicati nell'opzione *Indirizzo/i di inoltro*. Gli utenti di MDaemon che utilizzano l' accesso Web[347] con WorldClient[117] o WebAdmin[144] possono utilizzare le opzioni fornite per impostare le opzioni di inoltro autonomamente, anziché chiedere di farlo all'amministratore.

Indirizzo/i di inoltro (separare ogni indirizzo con una virgola)
Questo campo consente di indicare gli indirizzi e-mail ai quali inoltrare copie dei messaggi in entrata, man mano che questi pervengono all'account. Una copia di ogni nuovo messaggio in arrivo al server viene generata e inoltrata automaticamente all'indirizzo specificato in questo campo, purché sia stata selezionata l'opzione *L'account inoltra correntemente la posta*. Per specificare più indirizzi, utilizzare la virgola come separatore.

Conserva copia locale della posta inoltrata
Per impostazione predefinita, una copia di ogni messaggio inoltrato viene consegnata normalmente alla casella postale dell'utente locale. Se si deseleziona questa casella, non viene conservata alcuna copia locale.

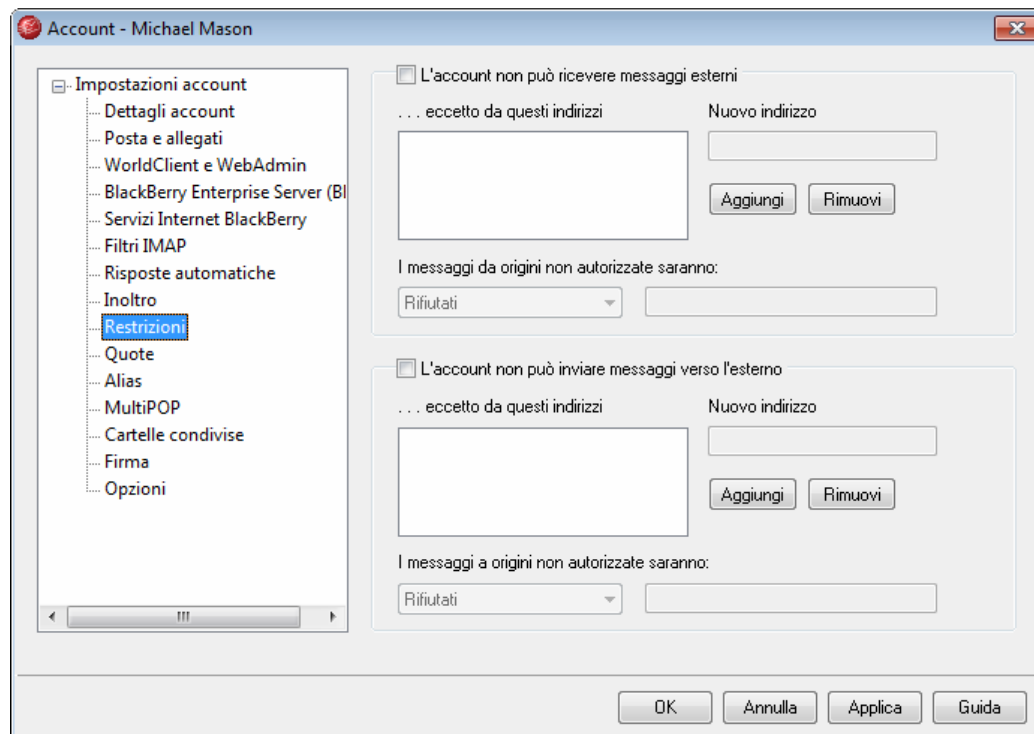
Opzioni di inoltro avanzate

Inoltra il messaggio a questo dominio
Se si desidera instradare i messaggi inoltrati tramite i server MX di uno specifico

dominio, questa casella consente di indicare il nome del dominio. Se si desidera instradare i messaggi verso un host specifico, racchiuderne il nome tra parentesi quadre, ad esempio `[host1.example.com])`.

Usa il seguente indirizzo nella busta SMTP
Se si specifica un indirizzo in questa casella, nell'istruzione "`MAIL From`" inviata durante la sessione SMTP con l'host di destinazione verrà utilizzato tale indirizzo anziché il mittente effettivo del messaggio. Se si desidera un'istruzione SMTP "`MAIL From`" vuota ("`MAIL FROM <>`") inserire la stringa "[trash]".

Usa questa porta TCP
MDaemon invierà i messaggi inoltrati mediante la porta TCP specificata in questa casella. Il valore predefinito della porta SMTP è 25.

6.1.1.9 Restrizioni

Le opzioni di questa schermata consentono di definire se l'account potrà o meno inviare o ricevere messaggi e-mail indirizzati o provenienti da domini non locali. L'opzione *Limita account a invio e ricezione di sola posta locale* della schermata Posta e allegati 377 di Valori predefiniti nuovo account consente di applicare in modo predefinito questa restrizione a tutti gli account.

Restrizioni posta in entrata

L'account non può ricevere messaggi esterni
Selezionare questa casella di controllo se si desidera impedire all'account di ricevere

messaggi e-mail provenienti da domini non locali.

...eccetto da questi indirizzi
Agli indirizzi specificati in quest'area non vengono applicate le restrizioni per la posta in entrata. I caratteri jolly sono accettati. Se si specifica "*@altn.com" come eccezione, tutti i messaggi in entrata provenienti da qualsiasi indirizzo di altn.com vengono accettati e recapitati all'account.

Nuovo indirizzo
Se si desidera aggiungere un'eccezione di indirizzo all'elenco Restrizioni posta in entrata, digitarla in questo campo e fare clic sul pulsante Aggiungi.

Aggiungi
Una volta immesso un indirizzo nel campo *Nuovo indirizzo*, fare clic su questo pulsante per aggiungere l'indirizzo all'elenco delle eccezioni.

Rimuovi
Se si desidera rimuovere un indirizzo dall'elenco delle restrizioni, selezionarlo e fare clic su questo pulsante.

I messaggi da origini non autorizzate saranno...
Le opzioni di questa casella di riepilogo a discesa specificano il comportamento di MDaemon per i messaggi destinati all'account ma provenienti da un dominio non locale o non autorizzato. È possibile scegliere una delle opzioni seguenti:

Rifiutati - I messaggi con restrizioni vengono rifiutati da MDaemon.

Restituiti al mittente - I messaggi provenienti dagli indirizzi con restrizioni vengono restituiti al mittente.

Inviati al postmaster - I messaggi con restrizioni vengono accettati ma recapitati al postmaster invece che all'account.

Inviati a...: i messaggi con restrizioni vengono accettati, ma consegnati all'indirizzo specificato nella casella di testo sulla destra.

Restrizioni posta in uscita

L'account non può inviare messaggi verso l'esterno
Selezionare questa casella di controllo se si desidera impedire all'account di inviare messaggi e-mail a domini non locali.

...eccetto da questi indirizzi
Agli indirizzi specificati in quest'area non si applicano le restrizioni per la posta in uscita. I caratteri jolly sono accettati. Se si specifica "*@altn.com" come eccezione, tutti i messaggi in uscita indirizzati a qualsiasi indirizzo di altn.com vengono recapitati normalmente.

Nuovo indirizzo
Se si desidera aggiungere un'eccezione di indirizzo all'elenco Restrizioni posta in uscita, digitare l'indirizzo in questione in questo campo, quindi fare clic sul

pulsante Aggiungi.

Aggiungi
Una volta immesso un indirizzo nel campo *Nuovo indirizzo*, fare clic su questo pulsante per aggiungere l'indirizzo all'elenco delle eccezioni.

Rimuovi
Se si desidera rimuovere un indirizzo dall'elenco delle restrizioni, selezionarlo e fare clic su questo pulsante.

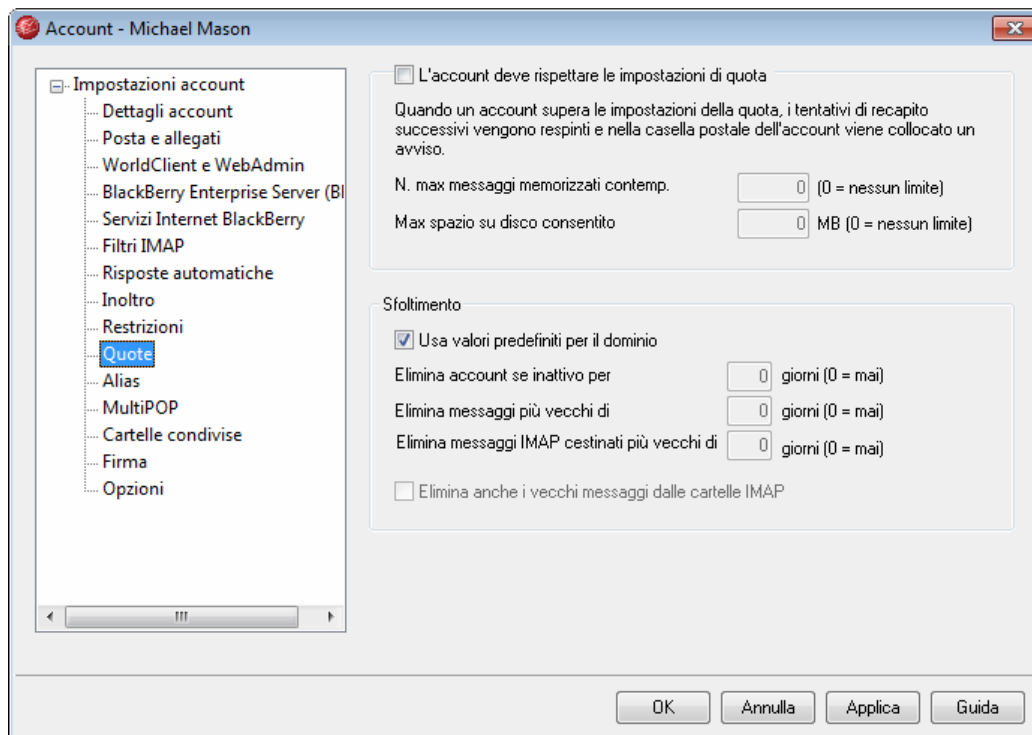
I messaggi indirizzati a origini non autorizzate saranno...
Le opzioni di questa casella di riepilogo a discesa specificano il comportamento di MDaemon per i messaggi provenienti dall'account ma indirizzati a un dominio non locale o non autorizzato. È possibile scegliere una delle opzioni seguenti:

Rifiutati - I messaggi destinati agli indirizzi non autorizzati vengono rifiutati da MDaemon.

Restituiti al mittente - I messaggi inviati agli indirizzi con restrizioni vengono restituiti al mittente.

Inviati al postmaster - I messaggi con restrizioni vengono accettati ma consegnati al postmaster invece che al destinatario designato.

Inviati a...: i messaggi con restrizioni vengono accettati, ma consegnati all'indirizzo specificato nella casella di testo sulla destra.

6.1.1.10 Quote

Opzioni quota

L'account deve rispettare le impostazioni di quota
Abilitare questa casella per specificare il numero massimo di messaggi da memorizzare nell'account o la quantità massima di spazio su disco utilizzabile dall'account, inclusi gli allegati dei file nella relativa cartella `\Files\`. Se si tenta di consegnare all'account una quantità di posta superiore ai limiti stabiliti per i messaggi e per lo spazio su disco, il messaggio viene respinto e nella casella postale dell'utente viene collocato un avviso appropriato. Se una raccolta MultiPOP supera il massimo consentito per l'account, viene emesso un avviso simile e le voci MultiPOP dell'account vengono disattivate automaticamente, ma non rimosse dal database.

L'opzione *Avviso per gli account che superano la percentuale della quota* di "Account » Impostazioni account » Quote 385" consente di inviare un messaggio di avviso quando un account sta per raggiungere i limiti definiti per le quote. Quando un account supera il valore percentuale indicato per il limite *Numero massimo di messaggi memorizzati contemporaneamente* o *Massimo spazio su disco consentito*, a mezzanotte riceve un messaggio di avviso. Nel messaggio verranno inclusi il numero di messaggi memorizzati, la dimensione della casella postale, la percentuale utilizzata e la percentuale rimanente. Se nella casella postale dell'account è già presente un messaggio di avviso, questo viene sostituito dal messaggio aggiornato.

Numero massimo di messaggi memorizzati contemporaneamente
Questa opzione consente di specificare il numero massimo dei messaggi che l'account può memorizzare. Il valore "0" indica che il numero di messaggi consentito è illimitato.

Massimo spazio su disco consentito
Questa opzione consente di indicare la quantità massima di spazio su disco utilizzabile dai nuovi account, inclusi gli allegati di file che è possibile memorizzare nella cartella `\Files\` dell'account. Il valore "0" indica che la quantità di spazio su disco consentita è illimitata.

Sfoltimento

Le opzioni di questa sezione consentono di specificare quando o se l'account verrà eliminato da MDaemon nel caso diventi inattivo. Consentono inoltre di indicare se i vecchi messaggi dell'account debbano essere eliminati dopo un determinato periodo di tempo. Ogni giorno a mezzanotte, MDaemon rimuove tutti i messaggi che hanno superato i limiti di tempo specificati o elimina completamente l'account, se questo ha raggiunto il limite di inattività.

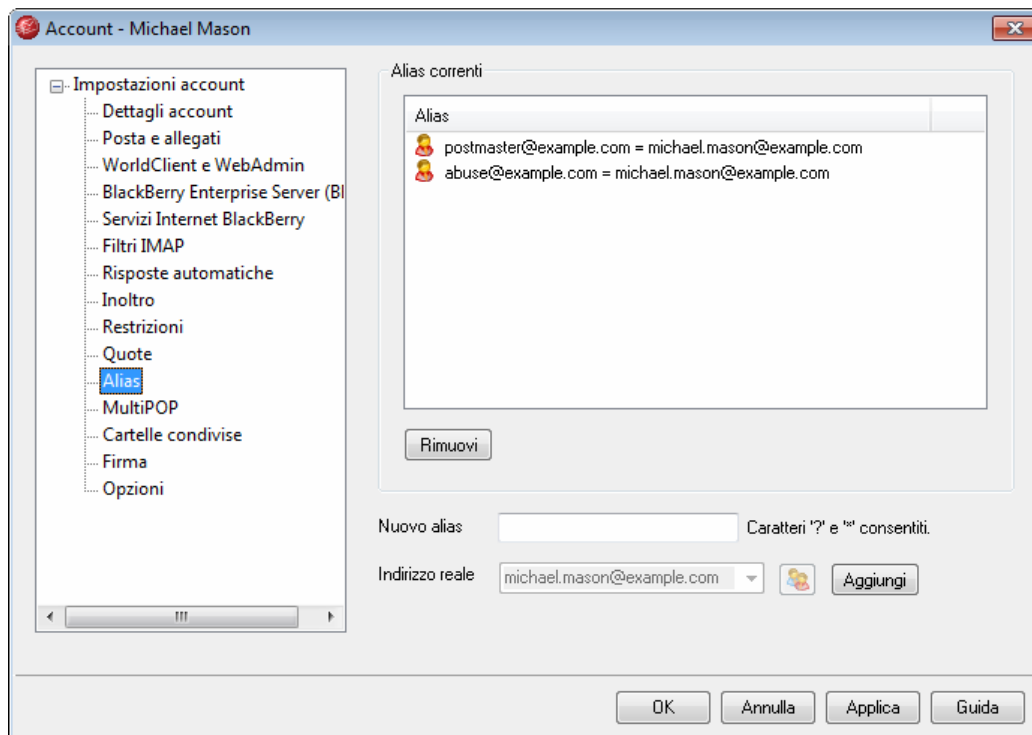
Usa valori predefiniti per il dominio
Le impostazioni di sfoltimento predefinite sono specifiche per i domini e sono situate in: Dominio predefinito/server » Sfoltimento 63 e Domini aggiuntivi 114. Per sovrascrivere le impostazioni predefinite di dominio per l'account, disabilitare questa casella di controllo e impostare i valori desiderati per le opzioni descritte di seguito.

Elimina account se inattivo per [XX] giorni (0 = mai)
Specificare il numero di giorni per cui si desidera che l'account rimanga inattivo prima di essere eliminato. Con il valore "0", un account non viene mai eliminato per inattività.

Elimina messaggi più vecchi di XX giorni (0 = mai)
Indica il numero di giorni per cui un determinato messaggio può rimanere nella casella postale dell'account prima di essere eliminato automaticamente da MDaemon. Il valore "0" indica che, anche se di vecchia data, i messaggi non vengono mai eliminati.

Elimina messaggi IMAP cestinati più vecchi di [XX] giorni (0 = mai)
Utilizzare questo comando per specificare il numero di giorni per cui si desidera che i messaggi IMAP contrassegnati per l'eliminazione rimangano nelle cartelle dell'utente. I messaggi contrassegnati per l'eliminazione da un numero di giorni superiore a questo valore vengono eliminati. Se si immette il valore "0", un messaggio vecchio contrassegnato per l'eliminazione non viene mai eliminato.

Elimina anche i vecchi messaggi dalle cartelle IMAP
Selezionare questa casella di controllo se si desidera applicare l'opzione "*Elimina i messaggi più vecchi di*" anche ai messaggi presenti nelle cartelle IMAP. Se questa opzione è disabilitata, i messaggi contenuti nelle cartelle IMAP non vengono eliminati, a prescindere dal periodo di permanenza nelle cartelle in questione.

6.1.1.11 Alias

Nella schermata sono elencati tutti gli alias 395 degli indirizzi associati con l'account ed è possibile effettuare aggiunte o rimozioni.

Rimozione di un alias

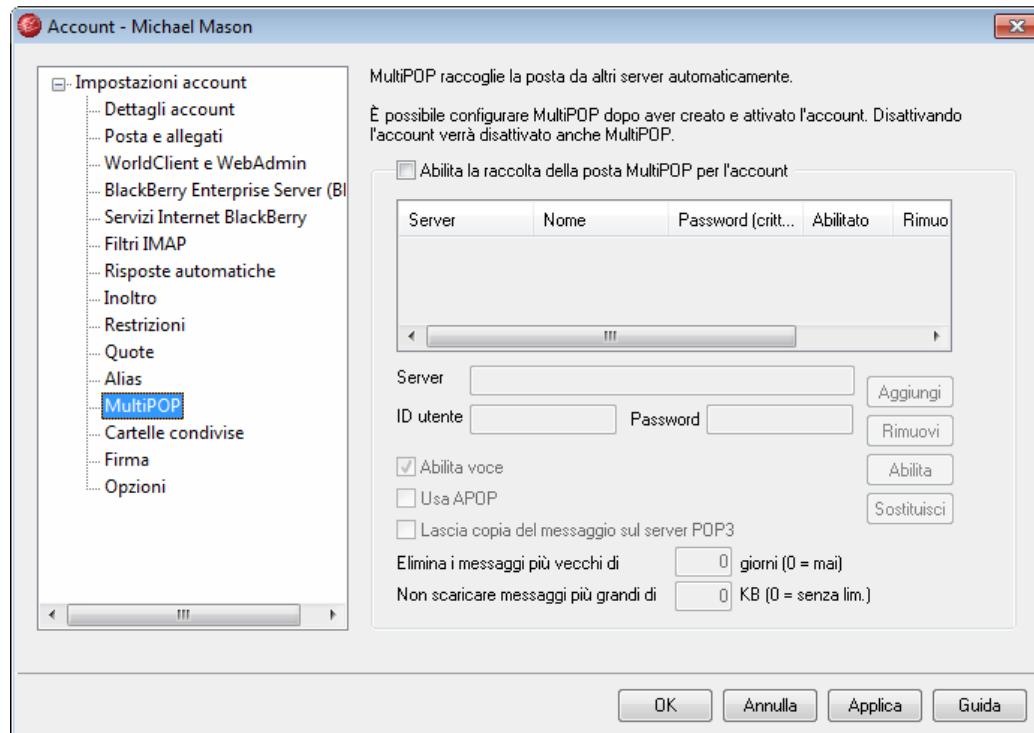
Per rimuovere un alias dall'account, selezionarlo nell'elenco e fare clic su **Rimuovi**.

Aggiunta di un alias

Per aggiungere un nuovo alias all'account, digitare nella casella *Nuovo alias* l'indirizzo che si desidera associare con l'account e fare clic su **Aggiungi.** Sono consentiti i caratteri jolly "?" e "*" che rappresentano, rispettivamente, singoli caratteri e singole parole.

Vedere:

Alias di indirizzo 395

6.1.1.12 MultiPOP

La funzione MultiPOP consente di creare un numero illimitato di combinazioni host/ utente/password POP3 per la raccolta di messaggi di posta provenienti da più origini. Si tratta di uno strumento utile per gli utenti che dispongono di account di posta su più server ma preferiscono raccogliere tutta la posta in un'unica postazione. Prima di essere collocata nella casella postale dell'utente, la posta MultiPOP raccolta viene inserita nella coda di posta per l'elaborazione, analogamente a tutti i messaggi per cui sono stati applicati la risposta automatica e i filtri di contenuto. Le opzioni di pianificazione della funzione MultiPOP sono disponibili in: Impostazioni » Pianificazione eventi » Opzioni di pianificazione posta » Raccolta MultiPOP 161.

Abilita la raccolta della posta MultiPOP per l'account
Abilitare questa casella per consentire l'elaborazione MultiPOP per l'account.

Elenco degli host MultiPOP dell'account
In questa casella viene visualizzato l'elenco di tutte le voci relative a host MultiPOP create per l'account.

Creazione o modifica di una voce MultiPOP

Server
Immettere il server POP3 da cui si desidera raccogliere la posta.

ID utente
Inserire il nome o l'ID utente POP3 associato all'account di posta del server specificato precedentemente.

Password
Immettere la password POP3 o APOP con cui accedere all'account di posta sul server specificato.

Usa APOP
Selezionare questa casella di controllo affinché la voce MultiPOP utilizzi il metodo di autenticazione APOP quando viene ritirata la posta dall'host corrispondente.

Lascia copia del messaggio sul server POP3
Selezionare questa casella di controllo per lasciare sul server una copia dei messaggi raccolti. Questa funzione è particolarmente utile se si prevede di ritirare in un secondo momento gli stessi messaggi da una postazione diversa.

Elimina messaggi più vecchi di XX giorni (0 = mai)
Specificare il numero di giorni per cui si desidera conservare i messaggi nell'host MultiPOP prima di eliminarli. Inserire "0" se non si desidera eliminare alcun messaggio.

Non scaricare messaggi più grandi di [XX] KB (0 = senza lim.)
Immettere un valore in questo campo per limitare la dimensione dei messaggi da scaricare.

Aggiungi
Dopo aver inserito tutte le informazioni relative alla nuova voce MultiPOP, per aggiungerla all'elenco fare clic su questo pulsante.

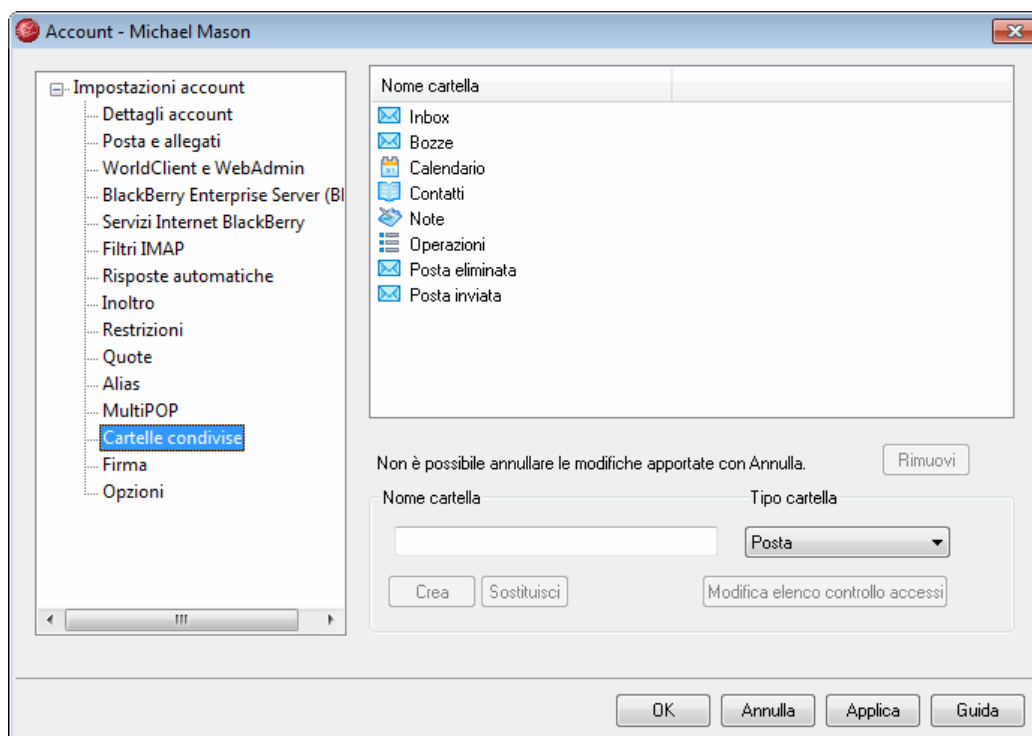
Rimuovi
Per eliminare una delle voci MultiPOP, selezionarla e fare clic su questo pulsante.

Abilita/disabilita
Facendo clic su questo pulsante, si attivano/disattivano le voci MultiPOP selezionate. Questa funzione consente di indicare a MDaemon di raccogliere la posta relativa a questa voce o di ignorarla quando esegue l'elaborazione MultiPOP.

Sostituisci
Se si desidera modificare una voce, selezionarla nell'elenco per visualizzarne le impostazioni tra le opzioni della schermata. Dopo aver apportato le modifiche, perché vengano applicate fare clic su questo pulsante.

Vedere:

Pianificazione eventi » Raccolta MultiPOP 161

6.1.1.13 Cartelle condivise

Questa schermata è disponibile solo se è stata selezionata l'opzione *Abilita cartelle condivise* della schermata Cartelle pubbliche e condivise 76, disponibile in Impostazioni » Dominio predefinito/server » Cartelle pubbliche e condivise.

Cartelle IMAP

La parte superiore consente di visualizzare tutte le cartelle IMAP dell'utente e può essere utilizzata per condividere l'accesso alle cartelle con altri utenti o gruppi di MDaemon. Quando l'account viene creato per la prima volta, l'area conterrà solo la cartella Posta in arrivo finché non si utilizzano le opzioni *Nome cartella* e *Crea* o le opzioni della scheda Filtri 353 per aggiungervi una cartella. Nelle sottocartelle presenti in questo elenco, i nomi della cartella e della sottocartella sono separati dal carattere barra "/".

Rimuovi

Per rimuovere dall'elenco una cartella IMAP condivisa, selezionarla e fare clic sul pulsante *Rimuovi*.

Nome cartella

Per aggiungere una nuova cartella all'elenco, immetterne il nome in questo campo e fare clic su *Crea*. Se si desidera che la nuova cartella sia una sottocartella di una di quelle in elenco, fare precedere al nome della nuova cartella il nome di quella principale e il carattere barra ("/"). Ad esempio, se la cartella principale è "Cartella personale", il nome della nuova sottocartella è "Cartella personale/Nuova cartella

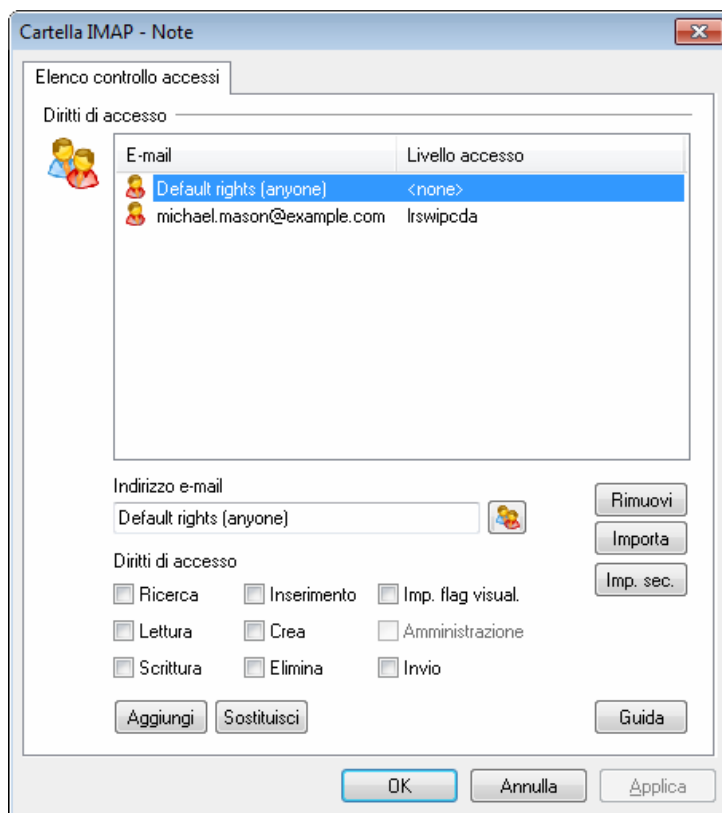
personale". Se non si desidera che la nuova cartella sia una sottocartella, assegnare il nome "Nuova cartella personale" senza il prefisso.

Tipo cartella
Utilizzare questo elenco a discesa per scegliere il tipo di cartella da creare: Posta, Calendario, Contatti e così via.

Crea
Una volta specificato il nome di una cartella, fare clic su questo pulsante per aggiungere la cartella all'elenco.

Sostituisci
Per modificare una delle cartelle condivise, selezionare la voce e apportare le modifiche desiderate, quindi fare clic su *Sostituisci.*.

Modifica elenco controllo accessi
Selezionare una cartella e fare clic su questo pulsante per aprire la finestra di dialogo Elenco controllo accessi 370 per la cartella. Utilizzare la finestra di dialogo Elenco controllo accessi per specificare gli utenti o i gruppi a cui sarà consentito accedere alla cartella, nonché le rispettive autorizzazioni.

6.1.1.13.1 Elenco controllo accessi

Diritti di accesso

In quest'area è possibile specificare gli account utente o i gruppi di MDaemon a cui si desidera accordare l'accesso alla cartella condivisa e impostare le relative autorizzazioni di accesso. La finestra di dialogo è disponibile nella schermata Cartelle condivise 369 di Account Editor. Per aprire la finestra di dialogo Elenco controllo accessi relativa a una cartella, fare doppio clic sulla cartella desiderata oppure selezionarla e successivamente fare clic su *Modifica elenco controllo accessi*. Ogni voce visualizza l'indirizzo e-mail dell'account e l'abbreviazione (composta da una lettera) del livello di accesso per ciascun diritto di accesso accordato all'utente.

Indirizzo e-mail
Digitare l'indirizzo e-mail oppure selezionare l'icona Account per selezionare l'account o il gruppo al quale si desidera accordare l'accesso alla cartella condivisa. Dopo aver indicato un account o un gruppo, selezionare i diritti di accesso desiderati e scegliere *Aggiungi* per aggiungere la voce all'elenco.

Rimuovi
Per rimuovere una voce dall'elenco dei diritti di accesso, selezionarla e fare clic sul pulsante *Rimuovi*.

Importa
La funzione *Importa* consente di aggiungere i membri di una lista di distribuzione già esistente all'elenco degli utenti con diritti di accesso. Scegliere i diritti di accesso che si desidera accordare agli utenti, fare clic su Importa, quindi fare doppio clic sulla lista desiderata. Tutti i membri della lista vengono aggiunti all'elenco con i diritti impostati.

Imp. sec.
Fare clic su *Imp. sec.* per applicare le autorizzazioni di controllo accessi della cartella a tutte le sue sottocartelle.

Diritti di accesso

Scegliere i diritti che si desidera accordare ai singoli utenti facendo clic sulle opzioni desiderate in quest'area, quindi fare clic su *Aggiungi* per le nuove voci o su *Sostituisci* per quelle esistenti.

È possibile accordare i diritti di controllo dell'accesso seguenti:

Ricerca (l) - L'utente è in grado di visualizzare la cartella nel proprio elenco personale di cartelle IMAP.

Lettura (r) - L'utente è in grado di aprire la cartella e visualizzarne il contenuto.

Scrittura (w) - L'utente è in grado di modificare i flag applicati ai messaggi della cartella.

Inserimento (i) - L'utente è in grado di allegare e copiare i messaggi nella cartella.

Creazione (c) - L'utente è in grado di creare delle sottocartelle della cartella.

Eliminazione (d) - L'utente è in grado di eliminare i messaggi dalla cartella.

Imp. flag. visual. (f) - L'utente è in grado di modificare lo stato letto/non letto dei messaggi presenti nella cartella.

Amministrazione (a) - L'utente è in grado di amministrare l'ACL (Access Control List) relativo alla cartella.

Invio (p) - L'utente è in grado di inviare la posta direttamente alla cartella, se quest'ultima lo consente.

Aggiungi
Dopo aver scelto dall'elenco un indirizzo e-mail o un gruppo e i diritti di accesso che si desidera accordare, fare clic su *Aggiungi* per aggiungere l'account o il gruppo all'elenco.

Sostituisci
Per modificare una voce di diritto di accesso esistente, selezionare la voce e apportare le modifiche desiderate al diritto di accesso, quindi fare clic su *Sostituisci*..

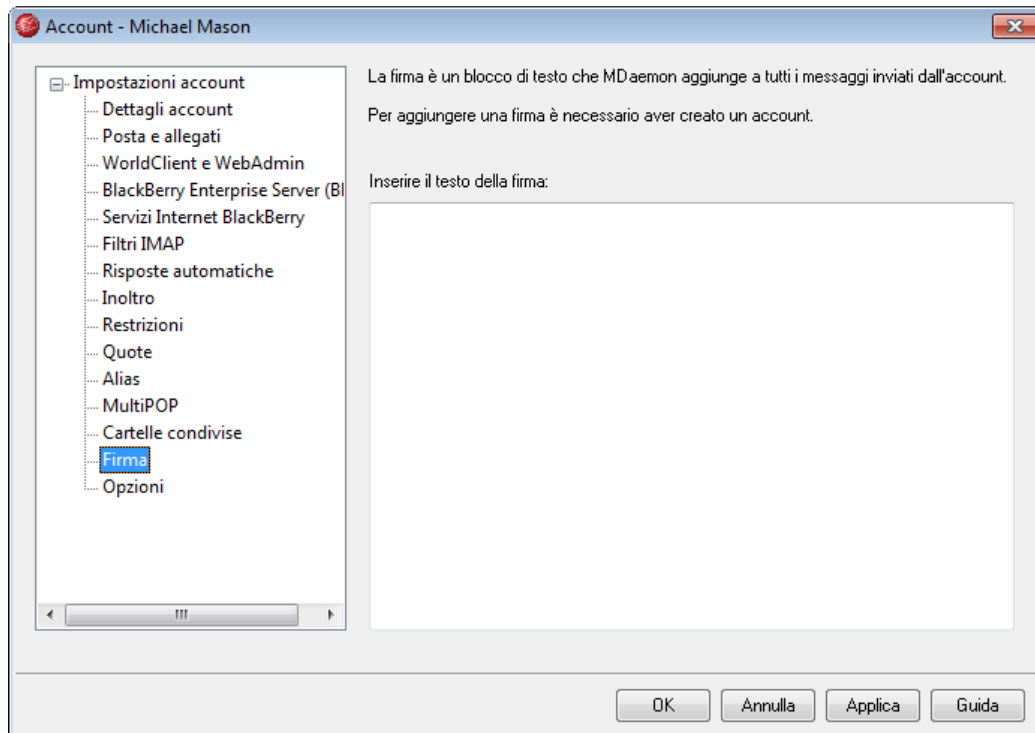
Guida
Fare clic su *Guida* per visualizzare un elenco dei diritti di accesso e delle relative definizioni.

I diritti di accesso vengono controllati mediante le funzioni di supporto ACL (Access Control List) di MDaemon. ACL è un'estensione del protocollo Internet Message Access Protocol (IMAP4) che rende possibile la creazione di un elenco di accessi per ognuna delle cartelle di messaggi IMAP esistenti, accordando i diritti di accesso alle cartelle anche ad altri utenti che dispongono di account sul server di posta. Se il client e-mail in uso non supporta ACL, è comunque possibile impostare le autorizzazioni mediante i comandi di questa finestra di dialogo.

Il protocollo ACL viene descritto approfonditamente nella RFC 2086, consultabile su Internet all'indirizzo http://www.rfc-editor.org/rfc/rfc2086.txt.

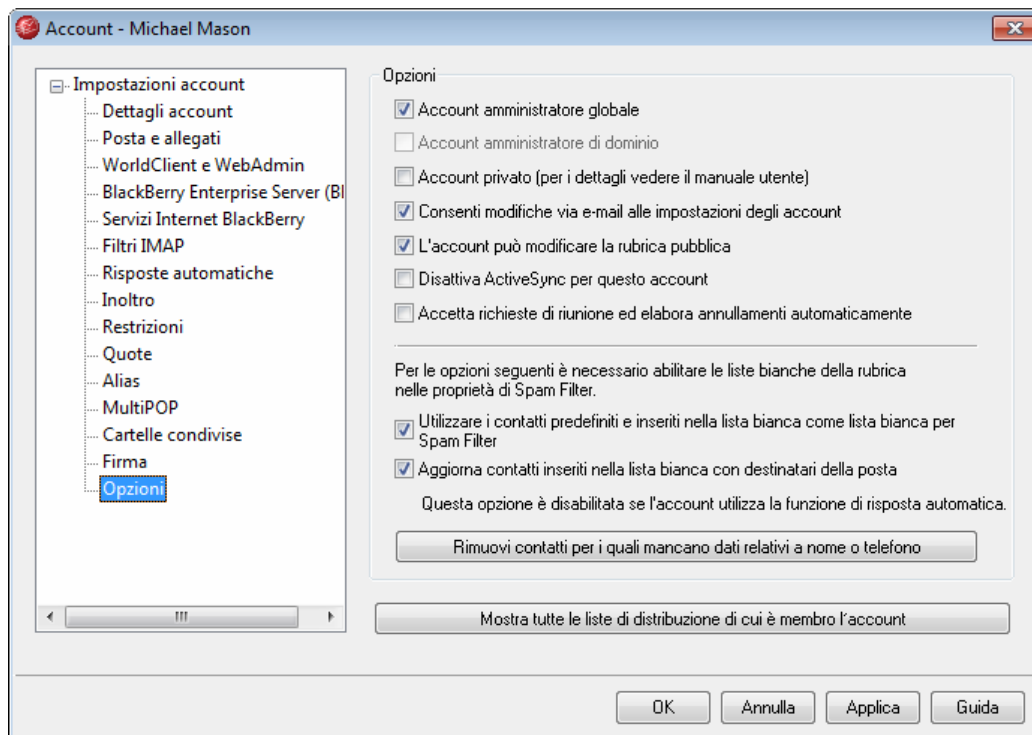
Vedere:

Account Editor » Cartelle condivise 369
Cartelle pubbliche e condivise 76
Elenco cartelle 78

6.1.1.14 Firma

Firma dell'account

Questa schermata consente di indicare una firma da allegare al termine di ogni e-mail inviata dall'account. Questa firma viene aggiunta alle altre firme o piè di pagina aggiunti mediante altre opzioni, come nel caso dell'opzione relativa alla firma di WorldClient e di altri client di posta, dell'opzione Firme di dominio 74 e dei piè di pagina delle liste di distribuzione 444. Le firme di dominio e i pié di pagina delle liste di distribuzione vengono sempre aggiunti successivamente alle firme dell'account.

Gli utenti in grado di accedere a WebAdmin 144 possono modificare la propria firma mediante le opzioni Account » firma disponibili in WebAdmin.

6.1.1.15 Opzioni

Opzioni

Account amministratore globale
Selezionare questa casella di controllo per concedere all'utente l'accesso al server a livello di amministratore. Agli amministratori globali sono associate le caratteristiche riportate di seguito.

- Accesso completo alla configurazione del server, a tutti gli utenti e a tutti i domini tramite WebAdmin
- Accesso agli utenti di tutti i domini di MDaemon come compagni di conversazione di messaggistica istantanea.
- Possibilità di inviare messaggi in tutte le liste di distribuzione anche se di sola lettura.
- Possibilità di inviare messaggi in tutte le liste di distribuzione anche non si è iscritti.

L'utente avrà inoltre accesso a tutti i file e opzioni di MDaemon. Per una descrizione delle opzioni amministrative di WebAdmin, consultare la sezione relativa a WebAdmin.

Account amministratore di dominio
Selezionare questa casella di controllo per designare l'utente come amministratore di dominio. Gli amministratori di dominio hanno privilegi simili a quelli degli amministratori globali, con l'unica differenza che l'accesso a livello amministrativo è limitato al dominio al quale appartengono. Per ulteriori informazioni sugli amministratori di dominio, vedere la sezione relativa a WebAdmin.

Account privato
MDaemon crea e gestisce automaticamente una lista di distribuzione "everyone@" per ogni dominio, utilizzabile per inviare un messaggio contemporaneamente a tutti i membri della lista. In base all'impostazione predefinita, quando crea questa lista di distribuzione MDaemon include tutti gli account. Questa casella consente di escludere l'account dalla lista. In tal modo, l'account viene escluso anche dai calendari condivisi e dai risultati VRFY 46.

Consenti modifiche via e-mail alle impostazioni degli account
Abilitando questa opzione, l'utente può accedere ai comandi relativi all'account che possono essere inclusi in messaggi e-mail appositamente formattati e inviati al server. Grazie a questa funzione, gli utenti possono eseguire le normali attività di manutenzione dell'account, quali la modifica del nome, della password, delle opzioni di inoltro e così via. Per una descrizione completa della modifica remota degli account tramite i messaggi e-mail, vedere: Controllo remoto del server via e-mail 506.

L'account può modificare la rubrica pubblica
Selezionare questa opzione per consentire all'account di aggiungere ed eliminare voci dalle rubriche di WorldClient o basate su LDAP.

Se è attiva la funzione di sincronizzazione delle cartelle dell'account mediante ComAgent, è possibile che le modifiche vengano estese a tutti gli utenti. Prestare molta attenzione quando si abilita questa funzione.

Disattiva ActiveSync per questo account
Selezionare questa casella per disabilitare ActiveSync per l'account. L'utente non sarà in grado di utilizzare ActiveSync su un dispositivo mobile per sincronizzare i propri dati relativi ai contatti e al calendario con MDaemon/WorldClient.

Accetta richieste di riunione ed elabora annullamenti automaticamente
Selezionare questa casella di controllo se si desidera abilitare l'elaborazione automatica delle richieste di riunione, delle modifiche e degli annullamenti per l'account. Se viene ricevuto un messaggio che contiene una richiesta di riunione, il calendario dell'account viene aggiornato automaticamente. Per impostazione predefinita, l'opzione è disabilitata per tutti gli account.

Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter
Nella schermata Lista bianca (automatica) 256 di Spam Filter è disponibile un'opzione globale che può essere utilizzata per evitare l'elaborazione di Spam Filter se il mittente di un messaggio è presente nella cartella dei contatti predefinita del destinatario locale o nella cartella della lista bianca personale. Questa opzione controlla tale funzionalità a livello di account. Se si è abilitata l'opzione globale di Spam Filter, ma non si desidera applicarla a questo account, deselezionare la casella di controllo.

Nota: ComAgent 120 consente facilmente di aggiornare e sincronizzare i contatti con WorldClient, la rubrica di Windows e altri client MAPI che utilizzano la rubrica di

Windows.

Aggiorna contatti inseriti nella lista bianca con destinatari della posta
Questa opzione consente di aggiornare la cartella della lista bianca dell'account ogni volta che questo invia un messaggio a indirizzi di posta elettronica remoti. Se utilizzata unitamente all'opzione *Utilizzare i contatti predefiniti e inseriti nella lista bianca come lista bianca per Spam Filter*, è possibile ridurre sensibilmente il numero di messaggi falsi positivi di Spam Filter. Per utilizzare questa funzione è necessario aver abilitato l'opzione *Aggiorna automaticamente i contatti inseriti nella lista bianca* della schermata Lista bianca (automatica)256.

Nota: questa opzione è disabilitata se l'account utilizza la funziona di risposta automatica.

Rimuovi contatti per i quali mancano dati relativi a nome o telefono
Questo pulsante consente di rimuovere dalla cartella Contatti predefinita dell'account tutti i contatti che contengono solo l'indirizzo di posta elettronica. I contatti privi del nome o dei dati telefonici vengono rimossi. Questa opzione è volta principalmente ad aiutare coloro che hanno utilizzato l'opzione della lista bianca automatica di MDaemon prima che la versione 11 eliminasse i contatti aggiunti solo in virtù della lista bianca. Nelle versioni di MDaemon precedenti, gli indirizzi venivano aggiunti ai contatti principali, anziché a una cartella lista bianca dedicata. Ciò può comportare un account con molte voci nella cartella dei contatti che sarebbe preferibile non avere.

È consigliabile utilizzare questa opzione con grande cautela, perché i contatti contenenti solo l'indirizzo di posta elettronica potrebbero essere legittimi.

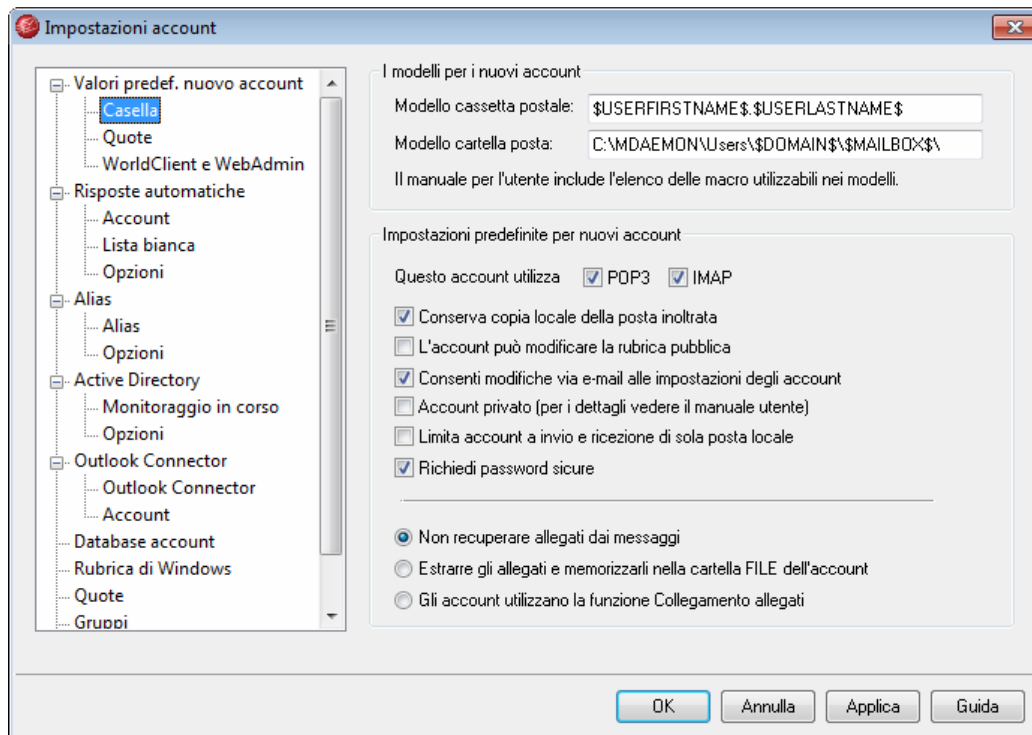
Mostra tutte le liste di distribuzione di cui è membro l'account
Questo pulsante consente di aprire l'elenco di tutte le liste di distribuzione428 cui l'account appartiene.

Vedere:

Lista bianca (automatica)256

6.2 Impostazioni account

6.2.1 Valori predefiniti nuovo account

6.2.1.1 Casella

Le opzioni di questa finestra di dialogo consentono di specificare i valori predefiniti di molte impostazioni relative agli account situate in Account Editor343. Le opzioni *Modello cassetta postale* e *Modello cartella posta*, inoltre, consentono di utilizzare numerose macro speciali381 per la generazione automatica degli indirizzi di posta elettronica e delle cartelle di memorizzazione della posta ogniqualvolta venga creato o importato un account. L'uso di questi modelli consente di semplificare e automatizzare la gestione dei nuovi account.

Modelli per i nuovi account

Modello cassetta postale
Questo campo consente di specificare un modello predefinito per il nome della casella postale dei nuovi account. Oltre a indicare la casella postale, questo valore costituisce il nome trasmesso unitamente al comando POP3 `USER` che consente l'accesso a una casella postale da una postazione remota o dai client di posta compatibili con POP. Per un elenco delle macro utilizzabili in questa stringa di modello, vedere Macro dei modelli381. "Per questa opzione, il modello predefinito è "`$USERFIRSTNAME$.$USERLASTNAME$`". Ad esempio, la creazione di un account per Franco Tommaso nel dominio esempio.com darà come risultato "`Franco.Tommaso@esempio.com`".

Modello cartella posta
Questo campo consente di specificare un modello predefinito per la cartella della posta dei nuovi account. La *cartella della posta* di ogni account rappresenta la posizione in cui vengono memorizzati i relativi messaggi e-mail nel server. È necessario accertarsi che, una volta espanso, il modello specificato formi un percorso valido.

MDaemon supporta un sistema di base di hashing delle cartelle. In NTFS, ad esempio, mantenere numerose cartelle sotto la stessa radice può avere un effetto negativo sulle prestazioni. Per limitare questo problema, è possibile utilizzare la macro `$MAILBOXFIRSTCHARSn$` in cui "`n`" è un numero compreso tra 1 e 10. La macro viene espansa ai primi "`n`" caratteri del nome della casella postale. Se si modifica il modello di directory della posta predefinita seguendo un metodo simile a quello riportato di seguito, sarà possibile ottenere un sistema di hashing delle cartelle sufficientemente valido:

```
C:
\MailboxRoot\$MAILBOXFIRSTCHARS4$\$MAILBOXFIRSTCHARS
2$\$MAILBOX$\.
```

Impostazioni predefinite per nuovi account

Queste opzioni vengono utilizzate per specificare i valori predefiniti di diverse impostazioni degli account. Per ulteriori informazioni, vedere Account Editor343.

Questo account utilizza

POP3
Per impostazione predefinita, gli account possono accedere ai propri messaggi e-mail tramite i client di posta POP3. Deselezionando questa casella, si impedisce a POP3 di accedere ai nuovi account per impostazione predefinita. Questa opzione determina l'impostazione predefinita dell'opzione POP3 situata nella schermata Dettagli account343 di Account Editor.

IMAP
Per impostazione predefinita, gli account possono accedere ai propri messaggi e-mail tramite i client di posta IMAP. Deselezionando questa casella, si impedisce a IMAP di accedere ai nuovi account per impostazione predefinita. Questa funzione è disponibile solo in MDaemon PRO. Questa opzione determina l'impostazione predefinita dell'opzione IMAP situata nella schermata Dettagli account343 di Account Editor.

Conserva copia locale della posta inoltrata
Per impostazione predefinita, se l'account utente è impostato per l'inoltro della posta MDaemon conserva una copia locale di ciascun messaggio in entrata nella relativa casella postale. Questa opzione determina l'impostazione predefinita dell'opzione corrispondente, situata nella schermata Inoltro360 di Account Editor.

L'account può modificare la rubrica pubblica
Questa opzione determina l'impostazione predefinita dell'opzione corrispondente, situata nella schermata Opzioni 374 di Account Editor. Selezionare questa opzione per consentire ai nuovi account di aggiungere ed eliminare voci dalle rubriche di WorldClient o basate su LDAP.

Se è attiva la funzione di sincronizzazione delle cartelle dell'account mediante ComAgent, è possibile che le modifiche vengano estese a tutti gli utenti. Prestare molta attenzione quando si abilita questa funzione.

Consenti modifiche via e-mail alle impostazioni degli account
Questa opzione determina l'impostazione predefinita dell'opzione corrispondente, situata nella schermata Opzioni 374 di Account Editor. Abilitando questa opzione, i nuovi utenti possono accedere ai comandi relativi all'account che possono essere inclusi in messaggi e-mail appositamente formattati e inviati al server. Grazie a questa funzione, gli utenti possono eseguire le normali attività di manutenzione dell'account, quali la modifica del nome, della password, delle opzioni di inoltro e così via. Per una descrizione completa della modifica remota degli account tramite i messaggi e-mail, vedere: Controllo remoto del server via e-mail 506.

Account privato
Questa opzione determina l'impostazione predefinita dell'opzione corrispondente, situata nella schermata Opzioni 374 di Account Editor. MDaemon crea e gestisce automaticamente una lista di distribuzione "everyone@" per ogni dominio, utilizzabile per inviare un messaggio contemporaneamente a tutti i membri della lista. In base all'impostazione predefinita, quando crea questa lista di distribuzione MDaemon include tutti gli account. Per nascondere o escludere i nuovi account dalla lista, abilitare questa casella di controllo. In tal modo, gli account vengono esclusi anche dai calendari e dai risultati VRFY 46.

Limita account a invio e ricezione di sola posta locale
Questa opzione determina l'impostazione predefinita delle due opzioni, situate nella schermata Restrizioni 361 di Account Editor. Se si abilita questa opzione, per tutti i nuovi account vengono abilitate entrambe le opzioni *L'account non può ricevere messaggi esterni* e *L'account non può inviare messaggi verso l'esterno* della finestra di dialogo. I nuovi account verranno limitati alla ricezione e all'invio della sola posta locale.

Richiedi password sicure
Per impostazione predefinita, in fase di creazione di nuovi account o di modifica delle password esistenti MDaemon richiede password sicure. Per disattivare la richiesta predefinita di password sicure, deselezionare questa casella di controllo.

È necessario che le password sicure:

- siano composte almeno dal numero di caratteri specificato (sei per impostazione predefinita);
- contengano sia lettere che numeri;

- includano lettere minuscole e maiuscole;
- non riportino informazioni relative alla casella postale o al nome completo.

Per indicare la lunghezza minima della password, modificare la seguente chiave di `MDaemon.ini`:

```
[Special]
MinPasswordLength=XX (impostazione predefinita 6)
```

Gestione degli allegati

Le altre tre opzioni corrispondono alle opzioni relative agli allegati che si trovano nella pagina Posta e allegati345 di Account Editor.

Non recuperare allegati dai messaggi
Con questa opzione, per impostazione predefinita, gli allegati non vengono estratti dai messaggi dell'account. I messaggi con allegati vengono gestiti normalmente e gli allegati rimangono invariati.

Estrarre gli allegati e memorizzarli nella cartella FILE dell'account
Se abilitata, questa opzione indica a MDaemon di estrarre automaticamente tutti gli eventuali file incorporati MIME Base64 allegati ai messaggi di posta in arrivo. I file estratti vengono rimossi dal messaggio in arrivo, decodificati e collocati nella sottocartella `\Files\`. Quindi, nel corpo del messaggio viene inserita una nota, con l'elenco dei nomi dei file estratti. Questa opzione non offre un collegamento agli allegati memorizzati, pertanto per recuperarli è necessario disporre dei diritti di accesso alla rete appropriati. Il livello di protezione e i requisiti utente per l'accesso ai file dipendono interamente dallo specifico sistema e dalle misure di sicurezza implementate.

Gli account utilizzano la funzione Collegamento allegati
Con questa opzione gli allegati vengono estratti dai messaggi in arrivo dell'account e memorizzati nella posizione indicata nella finestra di dialogo Collegamento allegati154. I collegamenti URL vengono quindi inseriti nel corpo del messaggio, dove è possibile selezionarli per scaricare i file. Per motivi di sicurezza, i collegamenti URL non contengono i percorsi diretti ai file. Contengono invece un identificativo univoco utilizzato dal server per mappare il file al percorso effettivo.

Se si disattiva globalmente questa funzione nella finestra di dialogo Collegamento allegati154, gli allegati non vengono estratti dai messaggi, indipendentemente dalle impostazioni selezionate.

Vedere:

[Macro dei modelli](381)
[Account Editor](343)
[Posta e allegati](345)
[Collegamento allegati](154)

6.2.1.1.1 Macro dei modelli

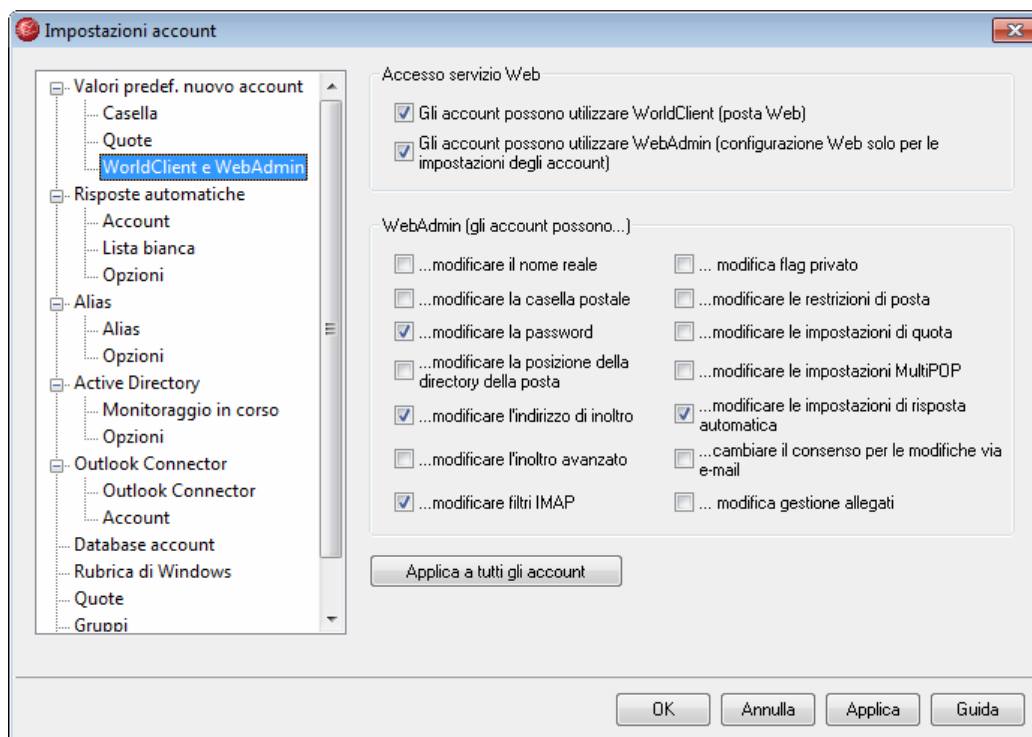
Di seguito è riportato un elenco di riferimento rapido di tutte le macro disponibili per l'automazione della configurazione degli account.

`$DOMAIN$`	Questa variabile viene sostituita dal nome di dominio selezionato per l'account.
`$DOMAINIP$`	Questa variabile viene sostituita dall'IP associato al dominio attualmente selezionato per l'account.
`$MACHINENAME$`	Questa macro restituisce il valore del campo relativo al nome del computer della scheda Dominio nella finestra di dialogo Dominio predefinito. La macro viene utilizzata per le nuove installazioni nello script contenente informazioni predefinite sugli account (NEWUSERHELP.DAT).
`$USERNAME$`	Questa variabile viene sostituita dal nome e cognome del titolare dell'account. Questo campo equivale a "$USERFIRSTNAME$ $USERLASTNAME$".
`$USERFIRSTNAME$`	Questa variabile viene sostituita dal nome del titolare dell'account.
`$USERLASTNAME$`	Questa variabile viene sostituita dal cognome del titolare dell'account.
`$USERFIRSTINITIAL$`	Questa variabile viene sostituita dalla prima lettera del nome del titolare dell'account.
`$USERLASTINITIAL$`	Questa variabile viene sostituita dalla prima lettera del cognome del titolare dell'account.

$MAILBOX$	Questa variabile viene sostituita dal nome della casella postale dell'account corrente. Il valore verrà utilizzato anche come valore del comando USER trasmesso durante le sessioni di posta POP3.
$MAILBOXFIRSTCHARSn$	Il valore "n" è un numero compreso tra 1 e 10. La macro viene sostituita con i primi "n" caratteri del nome della casella postale.

Per ulteriori informazioni, vedere:

Valori predefiniti nuovo account » Casella 377

6.2.1.2 WorldClient e WebAdmin

La schermata WorldClient e WebAdmin della finestra di dialogo Valori predefiniti nuovo account consente di specificare i diritti di accesso predefiniti a WorldClient 117 e WebAdmin 144 associati ai nuovi account. È possibile specificare se gli account possono accedere ai messaggi email mediante WorldClient e se gli utenti possono configurare i propri account mediante WebAdmin. Se si autorizza l'accesso a WebAdmin, è inoltre possibile controllare quali impostazioni possono essere modificate dagli account. Le opzioni di questa finestra di dialogo determinano le impostazioni predefinite delle opzioni corrispondenti situate nella schermata WorldClient e WebAdmin 347 di Account Editor.

Accesso servizio Web

Gli account possono utilizzare WorldClient (posta Web)
Selezionare questa casella di controllo se si desidera autorizzare i nuovi account ad accedere al server WorldClient 117, che consente di controllare l'e-mail mediante un browser Web.

Gli account possono utilizzare WebAdmin (config. Web solo per impost. account)
Abilitare questa casella per autorizzare i nuovi account alla modifica delle proprie impostazioni mediante WebAdmin 144. Gli utenti potranno modificare solo le impostazioni specificate successivamente.

WebAdmin (gli account possono...)

...modificare il nome reale
Abilitando questa funzione, i nuovi utenti possono modificare l'impostazione *Nome e cognome*.

...modificare la casella postale
Abilitando questa funzione, i nuovi utenti possono modificare la parte dell'*indirizzo e-mail* relativa alla propria casella postale.

Poiché il nome della casella postale fa parte dell'indirizzo e-mail dell'account e rappresenta l'identificativo univoco e il valore dell'ID utente utilizzato per l'accesso, modificarla significa modificare l'effettivo indirizzo e-mail dell'utente. Ciò può determinare il rifiuto, l'eliminazione o comunque la perdita dei futuri messaggi diretti al precedente indirizzo.

...modificare la password
Selezionare questa casella di controllo per consentire ai nuovi utenti di modificare la propria *Password e-mail.*

...modificare la posizione della directory della posta
Abilitando questa casella, i nuovi utenti vengono autorizzati a modificare la cartella dei messaggi 345 dell'account.

È opportuno prestare particolare cautela nel concedere questa autorizzazione. Infatti, la modifica della cartella dei messaggi consente di influire su tutte le cartelle del server.

...modificare l'indirizzo di inoltro
Quando questa funzione è abilitata, i nuovi utenti sono in grado di modificare le impostazioni dell'indirizzo di inoltro 360.

...modificare l'inoltro avanzato
Quando questa funzione è abilitata, i nuovi utenti sono in grado di modificare le *opzioni di inoltro avanzate.*

...modificare filtri IMAP
Questa opzione consente agli utenti di creare e gestire i propri filtri di posta 353.
Questa funzione è disponibile solo in MDaemon PRO.

...modificare flag privato
Questa opzione indica se l'utente può utilizzare WebAdmin per modificare l'opzione "*Account privato*" della schermata Opzioni 374 di Account Editor.

...modificare le restrizioni di posta
Questa casella di controllo consente di autorizzare i nuovi account alla modifica delle limitazioni relative alla posta in entrata e in uscita, situate nella schermata Restrizioni 361.

...modificare le impostazioni di quota
Con questa casella di controllo è possibile consentire agli account la modifica delle impostazioni relative alla quota 364.

...modificare le impostazioni MultiPOP
Selezionare questa casella di controllo per consentire ai nuovi account di aggiungere nuove voci MultiPOP 367 e di attivare/disattivare la raccolta di posta MultiPOP per tali voci.

...modificare le impostazioni di risposta automatica
Selezionare questa casella di controllo per consentire agli utenti di aggiungere, modificare o eliminare le risposte automatiche 357 per i propri account.

...cambiare il consenso per le modifiche via email
Selezionare questa casella di controllo per consentire agli utenti di modificare le *impostazioni dell'account* mediante messaggi e-mail con formattazione speciale 506.

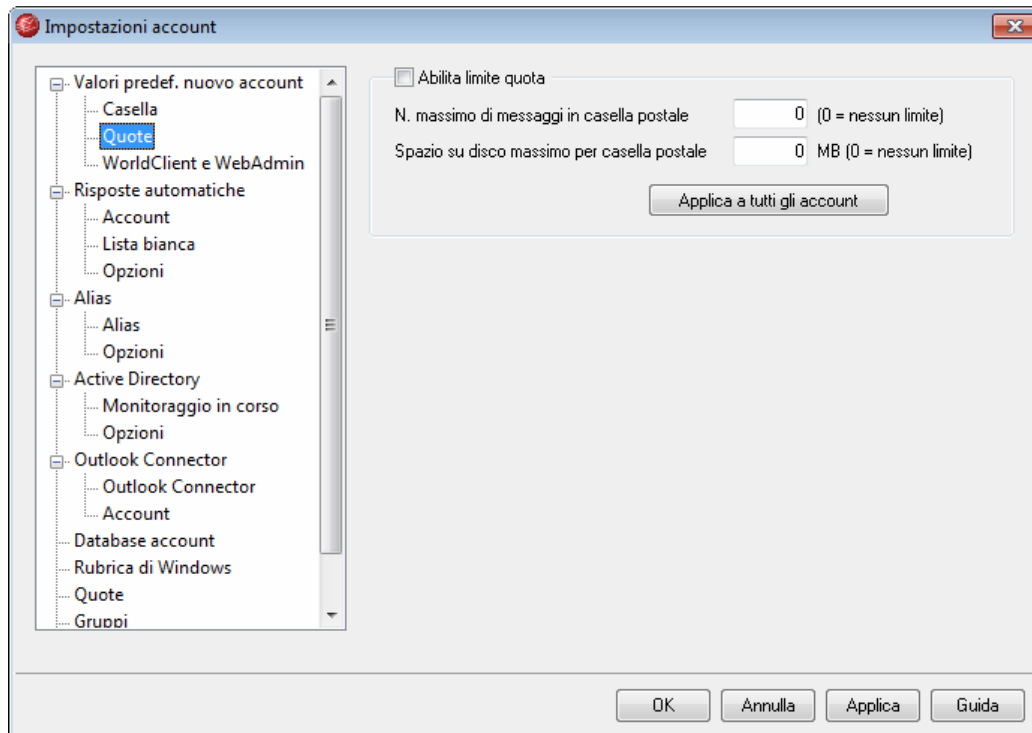
...modificare gestione allegati
Se si seleziona questa casella, l'utente ha la possibilità di modificare le opzioni di gestione degli allegati dell'account nella schermata Posta e allegati 345.

Applica a tutti gli account

Fare clic su questo pulsante per applicare le impostazioni di questa schermata a tutti gli account di MDaemon. In tal modo, gli account vengono reimpostati sui valori predefiniti per WorldClient e WebAdmin. Poiché questa azione è irreversibile, utilizzarla con cautela.

Vedere:

Account Editor » WorldClient e WebAdmin 347

6.2.1.3 Quote

In questa schermata è possibile indicare i valori predefiniti per le impostazioni relative alle quote degli account. Queste opzioni corrispondono a quelle di Quote 364 di Account Editor.

Quote

Abilita limite quota
Per impostare le quote di tutti i nuovi account, abilitare questa casella di controllo. È possibile specificare il numero massimo dei messaggi che gli account possono memorizzare e impostare la quantità massima di spazio su disco utilizzabile dagli account, inclusi gli allegati dei file delle cartelle `\Files\` di ogni account. Se si tenta di consegnare all'account una quantità di posta superiore ai limiti stabiliti per i messaggi e per lo spazio su disco, il messaggio viene respinto e nella casella postale dell'utente viene collocato un avviso appropriato. Se una raccolta MultiPOP supera il massimo consentito per l'account, viene emesso un avviso simile e le voci MultiPOP dell'account vengono disattivate automaticamente, ma non rimosse dal database.

L'opzione *Viene inviato messaggio di avviso se si arriva alla percentuale* di "Account » Impostazioni account » Quote 416" consente di inviare un messaggio di avviso quando un account sta per raggiungere i limiti definiti per le quote. Quando un account supera il valore percentuale indicato per il limite *N. massimo di messaggi in casella postale* o *Spazio su disco massimo per casella postale*, a mezzanotte riceve un messaggio di avviso. Nel messaggio verranno inclusi il numero

di messaggi memorizzati, la dimensione della casella postale, la percentuale utilizzata e la percentuale rimanente. Se nella casella postale dell'account è già presente un messaggio di avviso, questo viene sostituito dal messaggio aggiornato.

N. massimo di messaggi in casella postale
Questa opzione consente di specificare il numero massimo dei messaggi che i nuovi account possono memorizzare. Il valore "0" indica che il numero di messaggi consentito è illimitato.

Spazio su disco massimo per casella postale
Questa opzione consente di indicare la quantità massima di spazio su disco utilizzabile dai nuovi account, inclusi gli allegati di file che è possibile memorizzare nella cartella `\Files\` di ogni nuovo account. Il valore "0" indica che la quantità di spazio su disco consentita è illimitata.

Applica a tutti gli account

Fare clic su questo pulsante per applicare le impostazioni di questa schermata a tutti gli account di MDaemon. In tal modo, gli account vengono reimpostati sui valori delle quote predefiniti.

Vedere:

Account Editor » Quote 364
Impostazioni account » Quote 416

6.2.2 Risposte automatiche

6.2.2.1 Account

Le risposte automatiche sono strumenti che consentono, in base ai messaggi in entrata, di attivare eventi specifici quali l'esecuzione di un programma, l'inserimento di un mittente in una lista di distribuzione, l'invio di una risposta con un messaggio generato automaticamente e altro ancora. L'utilizzo più comune delle risposte automatiche consiste nella risposta automatica ai messaggi in entrata con un messaggio definito dall'utente con il quale viene comunicato che l'utente è in vacanza, non è disponibile, risponderà appena possibile e così via. Gli utenti di MDaemon che utilizzano l'accesso Web[347] con WorldClient[117] o WebAdmin[144] possono utilizzare le opzioni offerte per comporre i propri messaggi di risposta automatica e pianificarne le date. I messaggi di risposta automatica si basano su script di risposta, ossia file con estensione `*.RSP`, nei quali è possibile utilizzare numerose macro. Tali macro consentono la generazione dinamica di gran parte del contenuto degli script, rendendo le risposte automatiche particolarmente versatili.

Gli eventi di risposta automatica vengono utilizzati quando il messaggio di attivazione proviene da un'origine remota. Per i messaggi con origine locale, tuttavia, le risposte automatiche vengono attivate solo se è abilitata l'opzione *Risposte automatiche attivate da posta interna al dominio* della schermata Risposte automatiche » Opzioni[389]. Questa schermata consente inoltre di utilizzare un'opzione per limitare i messaggi di risposta automatica a una risposta al giorno per ogni mittente.

Elenco account

Quest'area include un elenco di tutte le caselle postali locali disponibili in grado di effettuare l'hosting delle risposte automatiche. Facendo doppio clic su un account verrà aperta la relativa schermata Risposte automatiche 357, nella quale è possibile configurare le risposte automatiche relative all'account.

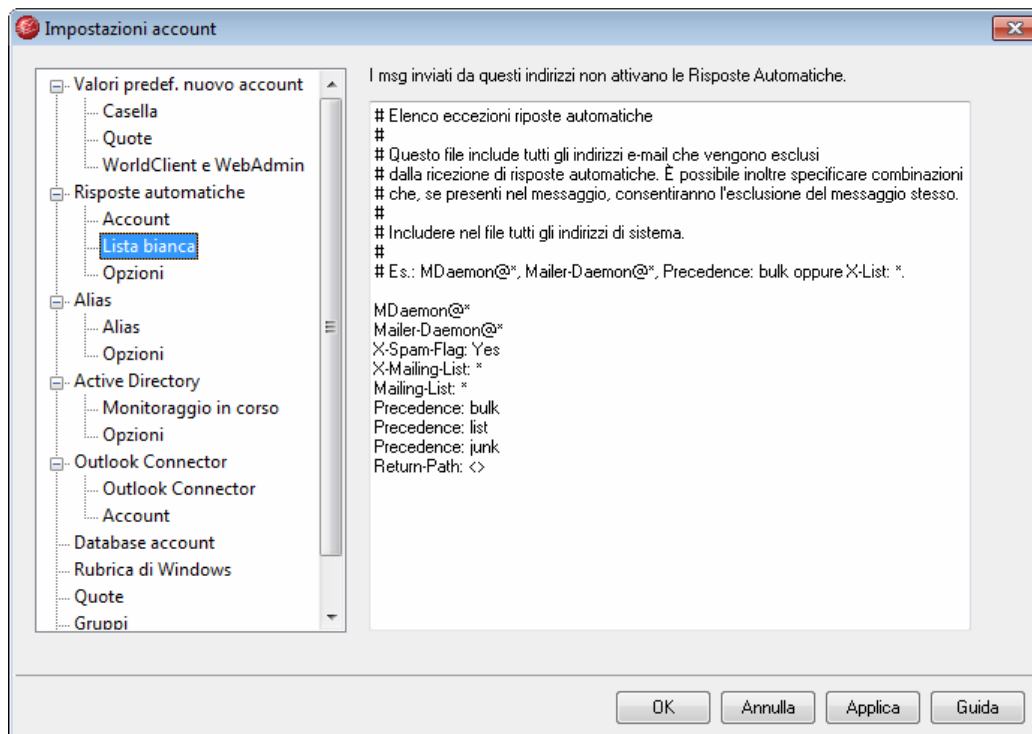
Vedere:

Risposte automatiche » Lista bianca 388

Risposte automatiche » Opzioni 389

Creazione degli script di risposta automatica 390

Account Editor » Risposte automatiche 357

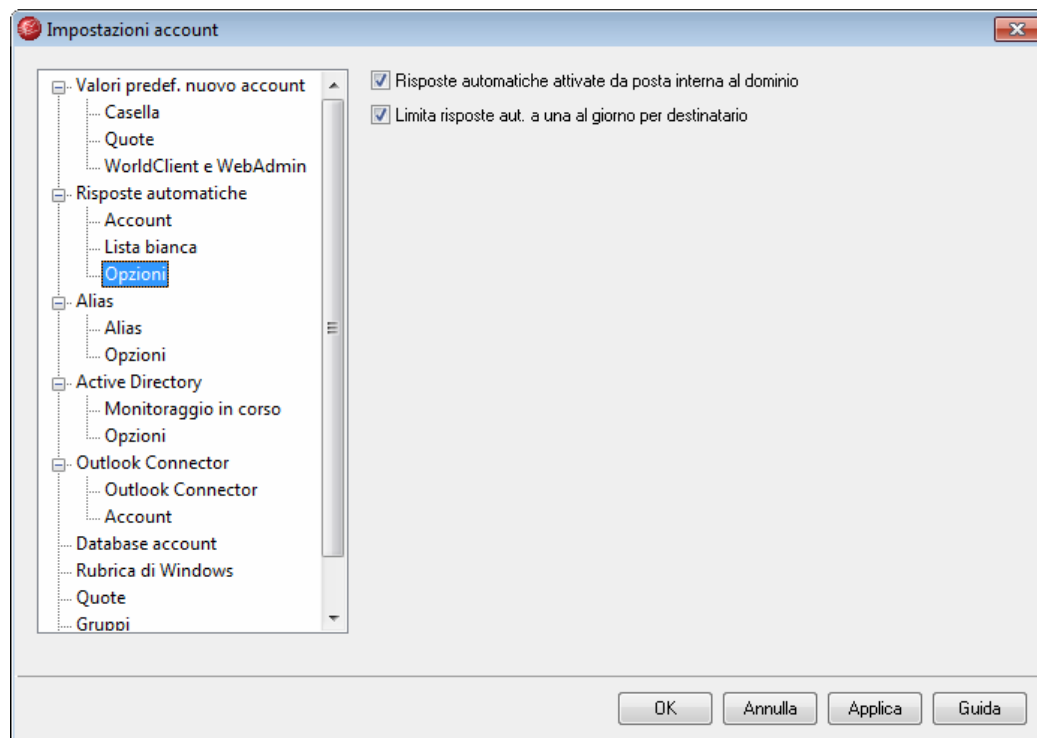
6.2.2.2 Lista bianca

Utilizzare Risposte automatiche » Lista bianca per configurare le eccezioni globali relative alle risposte automatiche. I messaggi delle voci nell'elenco non riceveranno alcuna risposta automatica. Nell'elenco possono essere inclusi sia indirizzi e-mail sia coppie intestazione/valore. Immettere un indirizzo o una coppia intestazione/valore per riga. I caratteri jolly sono accettati.

Per evitare la ripetizione dei cicli di posta e altri problemi, è necessario elencare tutti gli indirizzi di sistema, ovvero

mdaemon@*, mailer-daemon@* e così via.

Vedere:

Risposte automatiche » Account 387
Risposte automatiche » Opzioni 389
Creazione degli script di risposta automatica 390
Account Editor » Risposte automatiche 357

6.2.2.3 Opzioni

Opzioni

Risposte automatiche attivate da posta interna al dominio
Per impostazione predefinita, le risposte automatiche vengono attivate sia in modalità locale che in modalità remota. Se non si desidera che vengano attivate dalla posta inviata da un dominio locale di MDaemon, disabilitare questa casella.

Limita risposte aut. a una al giorno per destinatario
Per impostazione predefinita, le risposte automatiche generano un solo messaggio di risposta al giorno per un determinato indirizzo. In questo modo, si evita che il destinatario riceva lo stesso messaggio di risposta automatica più volte al giorno per ogni messaggio e-mail inviato. Per inviare una risposta automatica ad ogni messaggio ricevuto, anche se lo stesso mittente ne ha inviati più di uno al giorno, disabilitare

questa casella.

Questa opzione consente di prevenire i loop che possono verificarsi quando il messaggio di risposta automatica viene inviato a un indirizzo per il quale siano state attivate le risposte automatiche. Per evitare che gli indirizzi continuino a scambiarsi i messaggi di risposta, con questa opzione viene inviato a quell'indirizzo un solo messaggio al giorno.

Vedere:

Risposte automatiche » Account 387

Risposte automatiche » Lista bianca 388

Creazione degli script di risposta automatica 390

Account Editor » Risposte automatiche 357

6.2.2.4 Creazione degli script di risposta automatica

Gli script di risposta automatica sono file di testo che definiscono i messaggi restituiti come risultato di un evento di risposta automatica. Gli script vengono costruiti come file di testo ASCII semplice con estensione "*.rsp". Quando una risposta automatica attiva uno script, il file viene elaborato e analizzato alla ricerca di macro che, quindi, verranno sostituite dai dati effettivi del messaggio in entrata che ha attivato la risposta. Le righe che iniziano con il carattere "#" vengono ignorate, perché utilizzate per i commenti.

Di seguito sono elencati numerosi esempi di script, che si aggiungono ai numerosi file "*.rsp" generici presenti nella cartella \app\ di MDaemon.

Macro degli script di risposta automatica

$HEADERS$ Questa macro viene sostituita da tutte le intestazioni dei messaggi in entrata. Il testo immediatamente precedente la macro viene duplicato all'inizio di ogni riga espansa.

$HEADER:XX$ Questa macro determina l'espansione nel messaggio del valore dell'intestazione specificata al posto di "xx". Ad esempio: se nel messaggio originale è presente "TO: gianni@esempio.com", la macro $HEADER:TO$ verrà espansa in "gianni@esempio.com". Se nel messaggio originale è presente "SUBJECT: Questo è l'oggetto", la macro $HEADER:SUBJECT$ verrà sostituita dal testo "Questo è l'oggetto".

$BODY$ Questa macro viene sostituita dall'intero corpo del

messaggio. Nel tentativo di preservare i set caratteri di lingue diverse, MDaemon legge il corpo del messaggio come se si trattasse di dati binari anziché di testo semplice, consentendo una copia byte per byte del corpo del messaggio.

`$BODY-AS-TEXT$` Analogamente alla macro `$BODY$`, anche questa viene sostituita dall'intero corpo del messaggio, ma viene letta come testo semplice anziché come dati binari. Il testo immediatamente precedente la macro viene duplicato all'inizio di ciascuna riga espansa. Pertanto, l'utilizzo della macro "`>>$BODY-AS-TEXT$`" in uno script collocherà nel messaggio generato ogni riga del messaggio originale, preceduta da "`>>`". È possibile aggiungere testo anche a destra della macro.

`$ATTACHMENTS$` Questa macro viene sostituita dall'elenco completo di tutti i file allegati estratti dal messaggio originale. Il testo immediatamente precedente questa variabile di modello viene duplicato all'inizio di ogni riga espansa.

Ad esempio: `FILE-LIST: $ATTACHMENTS$` collocherà ciascun nome di file allegato nel messaggio generato, dopo la stringa di testo "`FILE-LIST:`".

`$ATTACHMENTCOUNT$` Questa macro viene sostituita da un valore intero uguale al numero di allegati estratti dal messaggio originale.

`$ATTACHMENT(X)$` Questa macro viene sostituita dal nome del file allegato associato al numero di allegato passato nel parametro X. Se il valore di X è maggiore del numero totale dei file allegati, l'intera variabile viene rimossa e non viene sostituita.

`$SENDER$` Questa macro viene sostituita dall'indirizzo completo presente nell'intestazione "`From:`" del messaggio in entrata.

`$SENDERMAILBOX$` Questa macro viene sostituita dalla casella postale del mittente. La casella postale è la porzione dell'indirizzo e-mail che si trova a sinistra del simbolo "@".

`$SENDERDOMAIN$` Questa macro viene sostituita dal dominio del mittente. Si tratta della porzione dell'indirizzo e-mail che si trova a destra del simbolo "@".

$RECIPIENT$	Questa macro viene sostituita dall'indirizzo completo del destinatario del messaggio.
$RECIPIENTMAILBOX$	Questa macro viene sostituita dalla casella postale del destinatario del messaggio. La casella postale è la porzione dell'indirizzo e-mail che si trova a sinistra del simbolo "@".
$RECIPIENTDOMAIN$	Questa macro viene sostituita dal dominio del destinatario del messaggio. Il dominio è la porzione dell'indirizzo e-mail che si trova a destra del simbolo "@".
$SUBJECT$	Questa macro viene sostituita dal valore dell'intestazione "`Subject:`".
$MESSAGEID$	Questa macro viene sostituita dal valore dell'intestazione "`Message-ID`".
$CONTENTTYPE$	Questa macro viene sostituita dal valore dell'intestazione "`Content-Type`".
$PARTBOUNDARY$	Questa macro viene sostituita dal valore MIME "Part-Boundary" presente nell'intestazione "`Content-Type`" dei messaggi multipart.
$DATESTAMP$	Questa macro viene sostituita da una riga di indicatore data-ora nel formato specificato da RFC-2822.
$ACTUALTO$	Alcuni messaggi possono contenere un campo "`ActualTo`" che, generalmente, rappresenta la casella postale e l'host di destinazione immessi dall'utente originale prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$ACTUALFROM$	Alcuni messaggi possono contenere un campo "`ActualFrom`" che, generalmente, rappresenta la casella postale e l'host di origine prima di qualsiasi riformattazione o conversione degli alias. Questa macro viene sostituita da tale valore.
$REPLYTO$	Questa macro viene sostituita dal valore dell'intestazione "`ReplyTo`".
$PRODUCTID$	Questa macro viene sostituita dalla stringa relativa alle informazioni sulla versione di MDaemon.

Macro per la sostituzione delle intestazioni

Le macro elencate di seguito controllano le intestazioni dei messaggi di risposta automatica.

%SetSender%
`Esempio: %SetSender%=casella postale@host.org`
Solo nel caso dei messaggi di risposta automatica, questa macro reimposta il mittente del messaggio originale prima di creare le intestazioni del messaggio di risposta automatica. Consente quindi di controllare l'intestazione `TO` del messaggio di risposta automatica. Se, ad esempio, il mittente del messaggio originale è "`pooky@dominio.com`" e la risposta automatica del destinatario ha utilizzato la macro `%SetSender%` per modificarlo in "`franco@esempio.com`", l'intestazione `TO` del messaggio di risposta automatica verrà impostata su "`franco@esempio.com`."

%SetRecipient%
Esempio: `%SetRecipient%=casellapostale@host.org`
Solo nel caso dei messaggi di risposta automatica, questa macro reimposta il destinatario del messaggio originale prima di creare le intestazioni del messaggio di risposta automatica. Consente quindi di controllare l'intestazione `FROM` del messaggio di risposta automatica. Se, ad esempio, il destinatario del messaggio originale è "`franco@esempio.com`" e la funzione di risposta automatica dell'account di Franco ha utilizzato la macro `%SetRecipient%` per modificarlo in "`franco.tommaso@esempio.com`," l'intestazione `FROM` del messaggio di risposta automatica verrà impostata su "`franco.tommaso@esempio.com`."

%SetReplyTo%
`Esempio: %SetReplyTo%=casella postale@host.org`
Controlla il valore dell'intestazione `ReplyTo` del messaggio di risposta automatica.

%SetActualTo%
`Esempio: %SetActualTo%=casellapostale@host.org`
Imposta il destinatario "effettivo" del messaggio.

%SetSubject%
`Esempio: %SetSubject%=Testo dell'oggetto`
Sostituisce il valore dell'oggetto del messaggio originale.

%SetMessageId%
`Esempio: %SetMessageId%=Stringa ID`
Modifica la stringa ID del messaggio.

%SetPartBoundary%
`Esempio: %SetPartBoundary%=Stringa Boundary`
Modifica il valore part-boundary.

%SetContentType%
`Esempio: %SetContentType%=Tipo MIME`
Modifica il tipo di contenuto del messaggio nel valore dichiarato.

%SetAttachment%
Esempio: `%SetAttachment%=filespec`
Impone a MDaemon di allegare il file specificato al messaggio di risposta automatica appena generato.

6.2.2.4.1 Esempi di script di risposta automatica

Un semplice script di risposta automatica, che utilizzi numerose macro di risposta automatica, potrebbe essere denominato `VACATION.RSP` e apparire come segue:

```
Caro $SENDER$

Non mi sarà possibile leggere il tuo messaggio riguardante
'$SUBJECT$' poiché sono in vacanza. Finalmente!!!
Cordialmente,

$RECIPIENT$
```

È inoltre possibile utilizzare alcune macro sostitutive delle intestazioni per espandere lo script e controllare le intestazioni generate quando il messaggio di risposta automatica viene reinviato a `$SENDER$`:

```
Caro $SENDER$

Non mi sarà possibile leggere il tuo messaggio riguardante
'$SUBJECT$' poiché sono in vacanza. Finalmente!!!
Cordialmente,

$RECIPIENT$

%SetSubject%=RE: $SUBJECT$
%SetAttachment%=c:\foto\mie_vacanze.jpg
```

Utilizzando questo script, viene aggiunto "`RE: `" all'inizio dell'oggetto del messaggio di risposta automatica e viene allegato il file indicato.

La riga "`%SetSubject%=RE: $SUBJECT$`" viene gestita come segue:

1. La porzione `$SUBJECT$` viene estesa e sostituita dal testo dell'oggetto del messaggio originale. La stringa pertanto risulta equivalente a:

   `%SetSubject%=RE: Testo dell'oggetto originale`

2. MDaemon sostituisce l'oggetto originale (memorizzato nei buffer interni) con quello appena calcolato. Successivamente, ogni volta che nello script verrà utilizzato "`$SUBJECT$`" si otterrà il nuovo risultato.

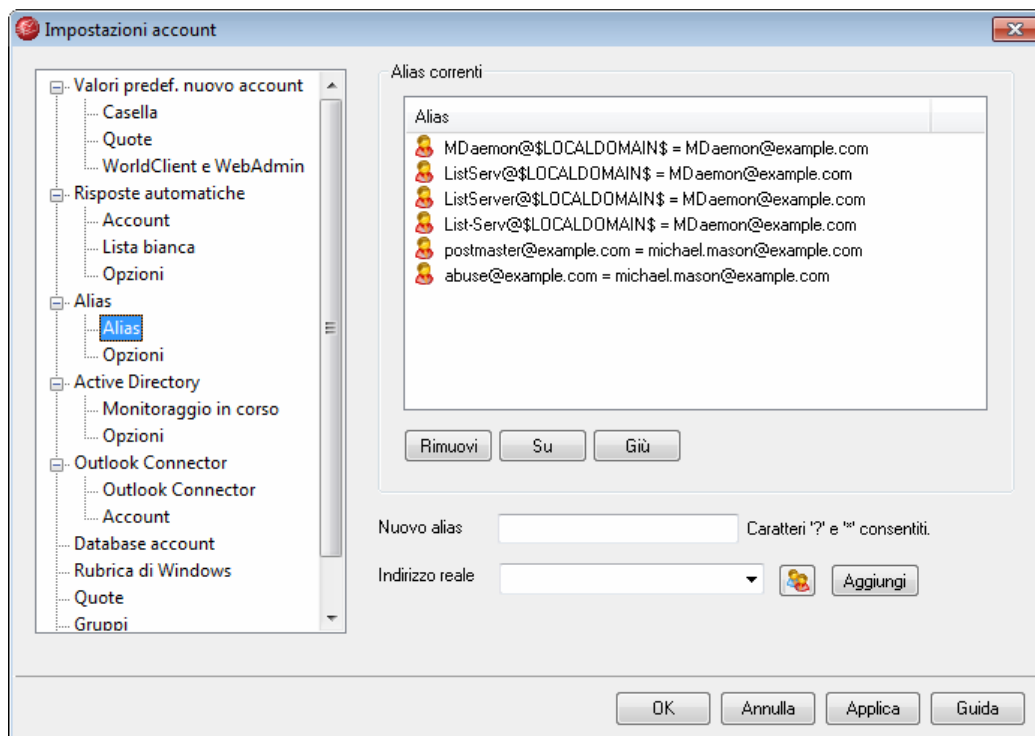
Si noti che le nuove macro sono elencate alla fine dello script di risposta, per evitare effetti collaterali. Se ad esempio la macro `%SetSubject%` fosse collocata prima della macro `$SUBJECT$`, visualizzata nella seconda riga dello script di risposta, il testo dell'oggetto verrebbe modificato prima dell'espansione della macro `$SUBJECT$`. Di conseguenza, anziché essere sostituita con il contenuto dell'intestazione `$SUBJECT$`

del messaggio originale, l'intestazione "`Subject:`" viene sostituita dal valore impostato per `%SetSubject%`.

Vedere:

Risposte automatiche » Account 387
Risposte automatiche » Lista bianca 388
Risposte automatiche » Opzioni 389
Account Editor » Risposte automatiche 357

6.2.3 Alias di indirizzo

6.2.3.1 Alias

Le opzioni relative agli alias, situate in Account » Impostazioni account, consentono di creare nomi di casella postale alternativi per gli account o le liste di distribuzione, utili quando si desidera che più nomi di caselle postali vengano risolti in un singolo account o lista utente. In assenza di alias è necessario creare account utente distinti per ogni indirizzo e, quindi, inoltrare i messaggi o utilizzare complesse regole filtro da associare agli altri account.

Se, ad esempio, `franco@esempio.com` gestisce tutte le richieste di fatturazione del proprio dominio, ma si desidera comunicare a tutti di inviarle a `fatturazione@esempio.com`, è possibile creare un alias affinché i messaggi indirizzati a `fatturazione@esempio.com` pervengano effettivamente a `franco@esempio.com`. In alternativa, se si ospitano più domini e si desidera che tutti i messaggi indirizzati al

postmaster, indipendentemente dal dominio, pervengano a franco@esempio.com, è possibile associare all'indirizzo un alias con un carattere jolly, ossia Postmaster@*.

Alias correnti

In questa finestra sono inclusi tutti gli alias creati.

Rimuovi
Questo pulsante consente di rimuovere una voce selezionata dall'elenco *Alias correnti*.

Su
Gli alias vengono elaborati in base alla posizione all'interno dell'elenco. È possibile spostare un alias in una posizione superiore selezionandolo e facendo clic su questo pulsante.

Giù
Gli alias vengono elaborati in base alla posizione all'interno dell'elenco. È possibile spostare un alias in una posizione inferiore selezionandolo e facendo clic su questo pulsante.

-

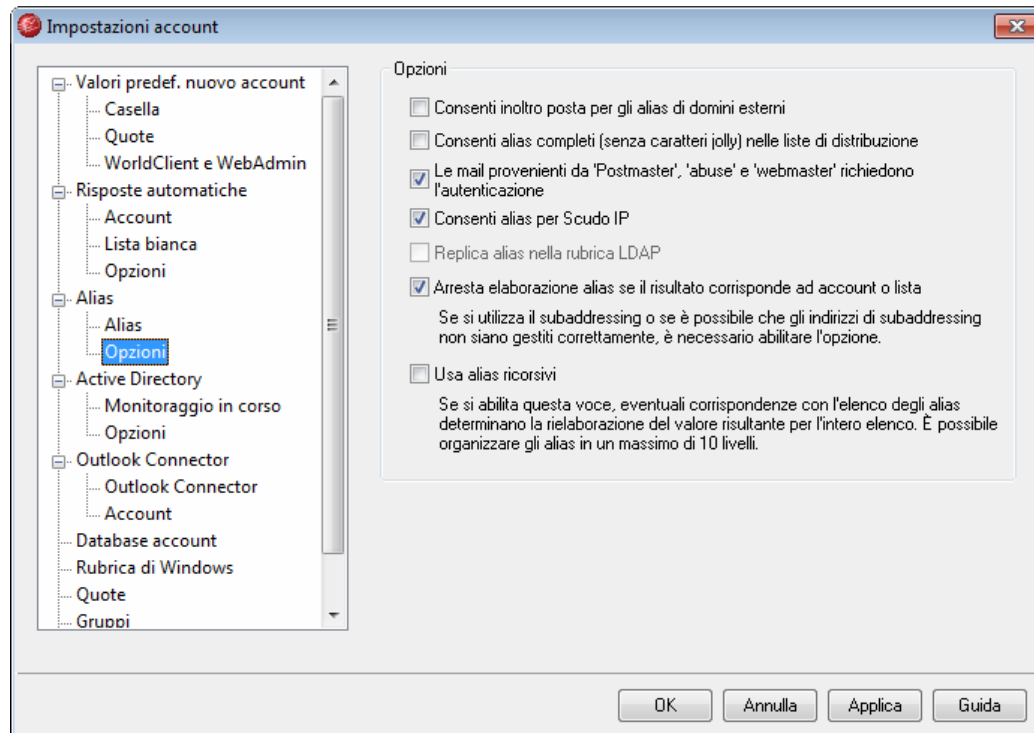
Nuovo alias
Inserire l'indirizzo email che si desidera come alias dell'*Indirizzo reale* indicato in precedenza. Sono consentiti i caratteri jolly "?" e "*" ed è possibile utilizzare "@$LOCALDOMAIN$" nell'alias come carattere jolly che corrisponde solo ai propri domini locali. Ad esempio: "franco@esempio.*", "*@$LOCALDOMAIN$" e "franco@$LOCALDOMAIN$" sono tutti alias ugualmente validi.

Indirizzo reale
Selezionare un account dall'elenco a discesa, utilizzare l'icona Account per individuare un account oppure digitare un nuovo indirizzo o una nuova lista di distribuzione. Si tratta dell'indirizzo che riceve effettivamente i messaggi indirizzati a un alias corrispondente.

Aggiungi
Per aggiungere l'alias all'elenco, fare clic sul pulsante *Aggiungi*. I valori di *Nuovo alias* e *Indirizzo reale* vengono combinati e inseriti nella finestra *Alias correnti*.

Vedere:

Alias » Opzioni 397
Account Editor » Alias 366

6.2.3.2 Opzioni

Opzioni

Consenti inoltro posta per gli alias di domini esterni
Abilitare questa casella di controllo per consentire a MDaemon di inoltrare la posta agli alias che comprendono domini non locali. Questa opzione ha la precedenza sull'opzione *Non consentire inoltro messaggi* di Controllo inoltro[274] relativa agli alias interessati.

Consenti alias completi (senza caratteri jolly) nelle liste di distribuzione
Selezionare questa casella di controllo per includere gli alias nelle liste di distribuzione di MDaemon. Se l'opzione è deselezionata, solo gli account reali potranno far parte di una lista di distribuzione. **Nota:** gli alias contenenti caratteri jolly non possono essere inclusi in una lista, anche se questa opzione è abilitata.

Le mail provenienti da 'postmaster', 'abuse' e 'webmaster' richiedono l'autenticazione
Abilitare questa opzione se si desidera che MDaemon richieda l'autenticazione dei messaggi che dichiarano di provenire dagli alias o dagli account "postmaster@...", "abuse@..." o "webmaster@..." prima di accettarli. Spammer e hacker sono a conoscenza della potenziale esistenza di tali indirizzi e possono, quindi, tentare di utilizzarli per inviare posta attraverso il sistema. Questa opzione consente di evitare questa eventualità. Per maggiore comodità questa opzione si trova anche nella schermata Autenticazione SMTP[283], disponibile in: Sicurezza » Impostazioni sicurezza. Qualsiasi modifica apportata in questa sede viene riportata anche nell'altra posizione.

Consenti alias per Scudo IP

Per impostazione predefinita, Scudo IP 276 accetta gli alias quando verifica i messaggi in entrata delle coppie dominio/IP valide. Con Scudo IP, l'alias viene convertito nell'account reale cui fa riferimento e, di conseguenza, viene accettato se il controllo ha esito positivo. Se questa opzione è disattivata, Scudo IP considera ogni alias come indirizzo indipendente dall'account che rappresenta. Di conseguenza, se l'indirizzo IP di un alias viola il controllo, il messaggio viene rifiutato. Questa opzione è duplicata nella schermata Scudo IP. Pertanto, se si modifica tale impostazione in questa sede, la modifica si rifletterà anche in quella.

Replica alias nella rubrica LDAP

Selezionare questa casella di controllo se si desidera che gli alias vengano replicati nella rubrica LDAP. La replica degli alias è necessaria affinché la funzione di verifica LDAP remota funzioni in modo affidabile. Tuttavia, se non si utilizza tale funzione, la replica nella rubrica LDAP non è necessaria. Se non si utilizza la verifica remota, è possibile disabilitare la funzione per ridurre il tempo di elaborazione. Per ulteriori informazioni sulla verifica LDAP remota, vedere LDAP 101.

Arresta elaborazione alias se il risultato corrisponde ad account o lista

Se si abilita questa opzione, l'elaborazione degli alias si arresta quando il destinatario del messaggio in entrata corrisponde a un account esistente o a una lista di distribuzione. Questa caratteristica fa riferimento in particolare agli alias che includono caratteri jolly. Se, ad esempio, un alias è impostato su "`*@esempio.com=franco@esempio.com`," con questa opzione l'alias viene applicato solo agli indirizzi che non esistono effettivamente nel server in uso. Se esiste l'account "`Enrico@esempio.com`", i messaggi indirizzati a Enrico vengono comunque recapitati all'utente perché l'alias non viene applicato a tali messaggi. Tuttavia, i messaggi indirizzati ad account inesistenti o a una lista verranno inviati a "`franco@esempio.com`" perché a questi messaggi viene applicato l'alias che include i caratteri jolly. L'opzione è abilitata per impostazione predefinita.

Quando si utilizza la funzione di subaddressing 355 è necessario abilitare questa opzione per evitare i potenziali problemi insiti nella gestione dei messaggi di questo tipo.

Usa alias ricorsivi

Selezionare questa casella di controllo se si desidera elaborare gli alias in modo ricorsivo. Se viene rilevata una corrispondenza di alias, il valore risultante verrà rielaborato attraverso l'intero elenco di alias. È possibile nidificare gli alias fino a 10 livelli. È ad esempio possibile specificare un'impostazione simile alla seguente:

```
adriano@esempio.com = franco@esempio.com
franco@esempio.com = x@x.com
x@x.com = dwimble@nome-esempio.net
```

Dal punto di vista logico, questa impostazione equivale al singolo alias:

```
adriano@esempio.com = dwimble@nome-esempio.net
```

Questi alias implicano inoltre che:

```
franco@esempio.com = dwimble@nome-esempio.net
```

Vedere:

Alias 395

6.2.4 Active Directory

Le opzioni relative ad Active Directory, disponibili in Account » Impostazioni account » Active Directory, consentono di configurare il monitoraggio di Active Directory al fine di creare, modificare, eliminare e disattivare automaticamente gli account MDaemon quando in Active Directory vengono modificati gli account associati.

Creazione degli account

Quando si imposta il monitoraggio di Active Directory, MDaemon esegue a intervalli prestabiliti interrogazioni relative alle modifiche e crea un nuovo account utente in MDaemon ogni qualvolta viene rilevata l'aggiunta di un nuovo account Active Directory. Tale nuovo account utente di MDaemon verrà creato utilizzando il nome completo, l'ID utente, la casella postale, la descrizione e lo stato attivo/inattivo riscontrato in Active Directory.

Per impostazione predefinita, i nuovi account MDaemon creati come risultato di un monitoraggio della Active Directory vengono aggiunti al dominio predefinito di MDaemon. In alternativa, è possibile scegliere di aggiungere questi account al dominio individuato in base all'attributo di Active Directory "`UserPrincipalName`" relativo all'account. Utilizzando questa opzione, se un account utilizza un dominio non ancora esistente in MDaemon, viene creato automaticamente un dominio aggiuntivo.

Eliminazione degli account

Nel caso di eliminazione di un account in Active Directory, è possibile configurare MDaemon affinché esegua una delle seguenti operazioni: non eseguire alcuna operazione, eliminare l'account di MDaemon associato, disattivare l'account di MDaemon associato oppure sospendere l'account di MDaemon associato. In quest'ultimo caso, l'account riceve ancora la posta ma l'utente non può raccoglierla né accedervi.

Aggiornamento degli account

Quando MDaemon rileva modifiche apportate agli account di Active Directory, eseguirà automaticamente un aggiornamento delle proprietà associate nel corrispondente account di MDaemon.

Sincronizzazione di MDaemon con la Active Directory

L'opzione "*Esegui scansione completa di AD*" consente di eseguire l'interrogazione del database di Active Directory e di creare o modificare, se necessario, gli account utente di MDaemon. Quando viene individuato un account di Active Directory che corrisponde ad un account MDaemon già esistente, i due account vengono collegati in modo che qualunque modifica futura dell'account Active Directory venga automaticamente apportata all'account MDaemon.

Autenticazione dinamica

Per impostazione predefinita, gli account creati dalla funzionalità Active Directory di MDaemon vengono impostati in modo da utilizzare l'autenticazione dinamica. Grazie a questa funzionalità, non è necessario che MDaemon memorizzi la password dell'account all'interno del database utenti. Il titolare dell'account utilizzerà le proprie credenziali Windows (ID utente e password) e MDaemon le trasferirà a Windows per l'autenticazione dell'account associato.

Per utilizzare l'autenticazione dinamica con Active Directory, è necessario che nel campo incluso in Monitoraggio 401 venga indicato un nome di dominio di Windows che corrisponde al dominio utilizzato da MDaemon al momento dell'autenticazione degli account. Nella maggior parte dei casi, MDaemon individua il nome di dominio Windows e compila automaticamente il campo. Tuttavia, se lo si desidera, è possibile specificare in questa opzione un dominio alternativo oppure indicare "NT_ANY" per consentire l'autenticazione di qualsiasi dominio Windows invece di limitarla ad uno specifico. Se questa opzione viene lasciata vuota, MDaemon non utilizzerà l'autenticazione dinamica alla creazione di nuovi account, ma genererà una password casuale da modificare manualmente prima che agli utenti sia consentito l'accesso ai relativi account di posta.

Monitoraggio permanente

Il monitoraggio di Active Directory viene eseguito anche quando MDaemon è inattivo. Tutte le modifiche apportate in Active Directory vengono registrate ed elaborate al riavvio di MDaemon.

Sicurezza dei file di Active Directory

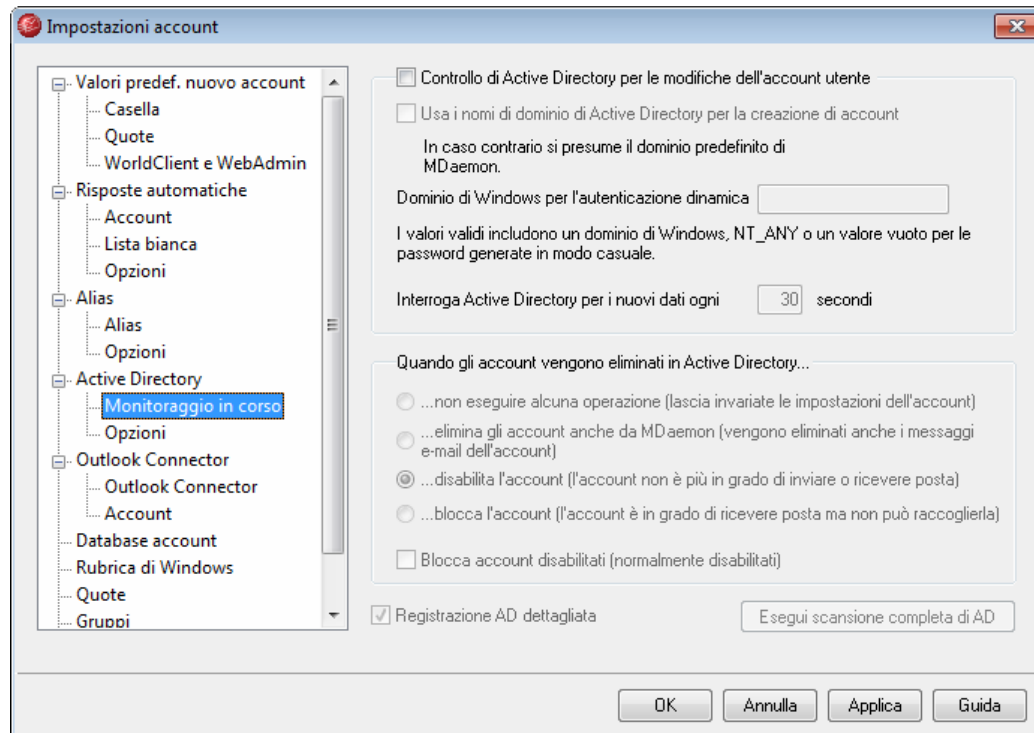
È importante notare che le funzionalità Active Directory di MDaemon non modificano i file di schema di Active Directory. Il monitoraggio è sempre a senso unico, da Active Directory a MDaemon .

Modello Active Directory

Ogni volta che vengono aggiunti o modificati account MDaemon a seguito del monitoraggio e della scansione di Active Directory, viene utilizzato un modello Active Directory ("/app/ActiveDS.dat") per collegare specifici nomi di attributi Active Directory ai campi relativi agli account di MDaemon. Ad esempio, per impostazione predefinita, MDaemon associa l'attributo "cn" di Active Directory al campo "FullName" di MDaemon. Questi collegamenti, comunque, non sono codificati rigidamente. Se lo si desidera, è possibile aprire il modello con Blocco note e modificare qualunque corrispondenza predefinita tra i campi. Ad esempio, è possibile utilizzare "FullName=%givenName% %sn%" per sostituire la seguente impostazione predefinita: "FullName=%cn%". Per ulteriori informazioni, consultare il file ActiveDS.dat.

Per ulteriori informazioni, vedere:

Active Directory » Monitoraggio 401
Active Directory » Opzioni 403

6.2.4.1 Monitoraggio

Active Directory

Controllo di Active Directory per le modifiche dell'account utente
Scegliere questa opzione per attivare il monitoraggio di Active Directory.

Usa i nomi di dominio di Active Directory per la creazione di account
Utilizzare questa opzione se si desidera aggiungere i nuovi account, creati a seguito del monitoraggio di Active Directory, al dominio specificato nell'attributo "`UserPrincipalName`" di Active Directory relativo all'account. Utilizzando questa opzione, se un account utilizza un dominio non ancora esistente in MDaemon, viene creato automaticamente un dominio aggiuntivo. Deselezionare/disattivare questa opzione se si desidera aggiungere tutti i nuovi account al dominio primario di MDaemon.

Dominio di Windows per l'autenticazione dinamica
Inserire in questo campo un nome di dominio Windows se si desidera utilizzare l'autenticazione dinamica per gli account creati dal monitoraggio di Active Directory. Se questo campo viene lasciato vuoto, ai nuovi account verranno assegnate password casuali che dovranno essere modificate manualmente per rendere accessibili gli account.

Interroga Active Directory per i nuovi dati ogni XX secondi
Rappresenta l'intervallo di tempo trascorso il quale MDaemon esegue un nuovo monitoraggio di Active Directory al fine di individuare eventuali modifiche.

Quando gli account vengono eliminati in Active Directory:
Quando un account MDaemon associato ad un account Active Directory viene eliminato, MDaemon esegue una determinata operazione, a seconda dell'opzione selezionata.

...non eseguire alcuna operazione
Scegliere questa opzione se non si desidera che MDaemon apporti modifiche all'account MDaemon quando l'account associato viene eliminato da Active Directory.

... elimina gli account anche da MDaemon
Scegliendo questa opzione, l'account MDaemon sarà eliminato insieme all'account associato di Active Directory.

In questo caso, l'account MDaemon associato verrà rimosso completamente. Saranno eliminati anche i messaggi dell'account, le cartelle, le rubriche, i calendari e così via.

...disabilita l'account
Se si seleziona questa opzione, quando un account viene eliminato in Active Directory il corrispondente account MDaemon viene disabilitato. In tal caso, l'account MDaemon continua a esistere sul server, ma non è possibile utilizzarlo per inviare o per ricevere la posta, né accedere all'account stesso.

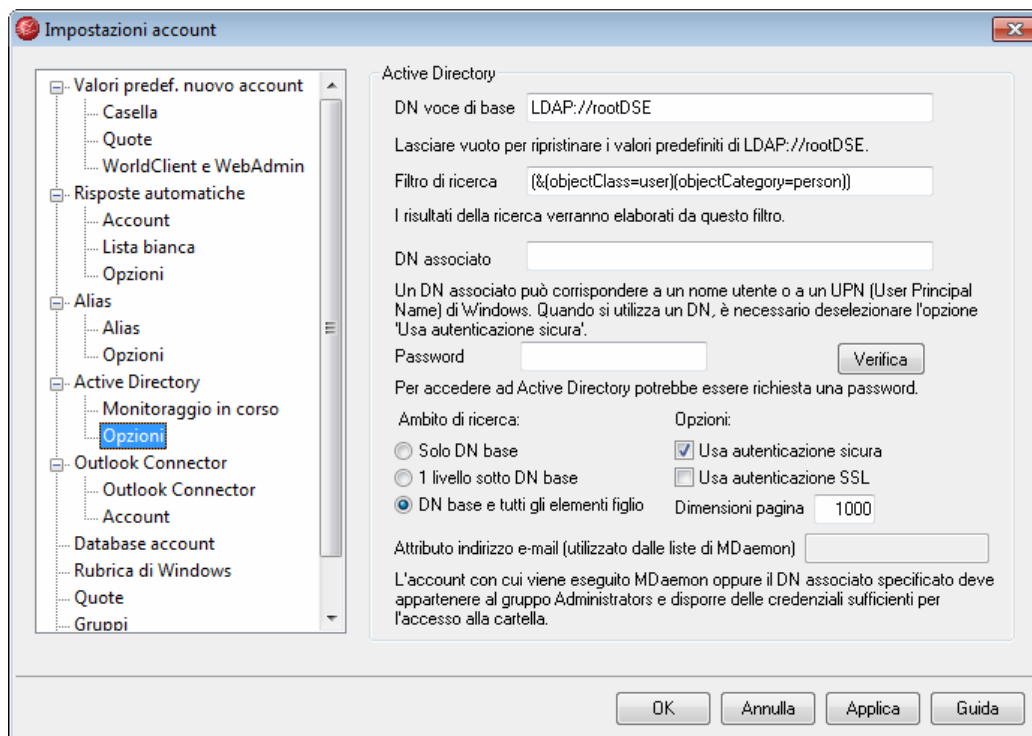
...blocca l'account
Selezionando questa opzione, è ancora possibile accettare la posta in entrata ma questa risulta "bloccata" e non è possibile quindi accedervi. In altre parole, la posta in arrivo indirizzata all'account non viene rifiutata o eliminata da MDaemon, ma il proprietario dell'account non è in grado di accedervi o di raccoglierla finché l'account rimane bloccato.

Blocca account disabilitati
Per impostazione predefinita, se un account viene disabilitato in Active Directory, viene disabilitato anche l'account MDaemon associato. In questo modo, l'account risulta inaccessibile e i messaggi indirizzati all'account non vengono accettati né consegnati da MDaemon. Tuttavia, se si desidera che l'account MDaemon associato venga bloccato anziché disabilitato, è possibile scegliere/attivare questa opzione. MDaemon continuerà ad accettare i messaggi destinati agli account bloccati, ma gli utenti non potranno accedere a tali account per raccogliere o per inviare la posta.

Registrazione AD dettagliata
Per impostazione predefinita, MDaemon utilizzerà la registrazione dettagliata per gli eventi di Active Directory. Deselezionare questa casella di controllo se si desidera utilizzare una modalità di registrazione meno dettagliata.

Esegui scansione completa di AD
Fare clic su questo pulsante per consentire a MDaemon di interrogare il database di Active Directory e, se necessario, creare, modificare o eliminare gli account. Quando viene individuato un account di Active Directory che corrisponde ad un account

MDaemon già esistente, i due account vengono collegati.

6.2.4.2 Opzioni

Per consentire l'utilizzo di tutte le funzionalità relative all'accesso ad Active Directory potrebbe essere necessario impostare autorizzazioni speciali.

Opzioni Active Directory

DN voce di base

Rappresenta il DN (Distinguished Name), ossia il punto iniziale nella struttura DIT (Directory Information Tree) a partire dal quale MDaemon esegue la ricerca degli account e delle modifiche apportate all'interno di Active Directory. Per impostazione predefinita, MDaemon esegue la ricerca a partire dal Root DSE, che consiste nella voce di livello più alto nella gerarchia della Active Directory. L'indicazione di un punto iniziale più accurato e prossimo alla posizione dell'account nella struttura Active Directory può ridurre il tempo necessario per la ricerca degli account e delle modifiche apportate all'account. Lasciando vuoto questo campo, verrà ripristinata l'impostazione predefinita `LDAP://rootDSE`

Filtro di ricerca

Rappresenta il filtro di ricerca LDAP utilizzato quando si esegue il monitoraggio o la ricerca di account e delle relative modifiche in Active Directory. Utilizzare questo

filtro per localizzare in modo più accurato gli account utente da includere nel monitoraggio di Active Directory.

DN associato
Rappresenta il DN utilizzato da MDaemon per l'associazione ad Active Directory mediante LDAP. Per l'associazione, Active Directory consente l'uso di un account Windows o di un UPN.

Quando si utilizza un DN invece di un ID utente Windows, in questa opzione è necessario disattivare/deselezionare l'opzione "*Utilizza autenticazione sicura*".

Password
È la password corrispondente al DN o all'ID utente Windows indicato nell'opzione *DN associato*.

Verifica
Fare clic su questo pulsante per eseguire una verifica della configurazione Active Directory di MDaemon.

Ambito di ricerca:

Rappresenta l'ambito, ossia la portata delle ricerche Active Directory.

Solo DN base
Scegliere questa opzione se si desidera limitare la ricerca al solo DN base indicato in precedenza. In questo modo, la ricerca nella struttura DIT non verrà eseguita oltre tale punto.

1 livello inferiore al DN base
Utilizzare questa opzione se si desidera estendere la ricerca nella struttura DIT di Active Directory ad un livello inferiore al DN specificato.

DN base e tutti gli elementi figlio
Con questa opzione, l'ambito della ricerca viene esteso dal DN fornito a tutti i relativi figli, fino all'ultimo elemento figlio del DIT. È l'opzione selezionata per impostazione predefinita che consente, se combinata con l'impostazione relativa alla directory principale DSE indicata in precedenza, di eseguire la ricerca nell'intera struttura DIT sottostante alla directory principale DSE.

Opzioni:

Usa autenticazione sicura
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione sicura durante l'esecuzione di ricerche in Active Directory. Non è possibile utilizzare questa opzione se nell'opzione *DN associato* indicata in precedenza viene specificato un DN anziché un ID utente Windows.

Usa autenticazione SSL
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione SSL

durante l'esecuzione di ricerche in Active Directory.

L'utilizzo di questa opzione richiede la presenza di un server e di un'infrastruttura SSL nella rete Windows e in Active Directory. Se non si è certi dell'impostazione della rete o per ulteriori informazioni sulla possibilità di attivare questa opzione, rivolgersi al proprio reparto IT.

Dimensioni pagina
Se l'interrogazione di Active Directory restituisce un numero elevato di voci, queste vengono raggruppate in "pagine" diverse per consentire il recupero di tutti i risultati. Questa impostazione rappresenta il numero massimo di voci da includere per ogni pagina.

Attributo indirizzo e-mail

Questo attributo è utilizzato nel caso delle liste di distribuzione di MDaemon ed è disponibile solo se si accede alle opzioni Active Directory nella finestra di dialogo Liste di distribuzione 446.

6.2.5 Outlook Connector per MDaemon

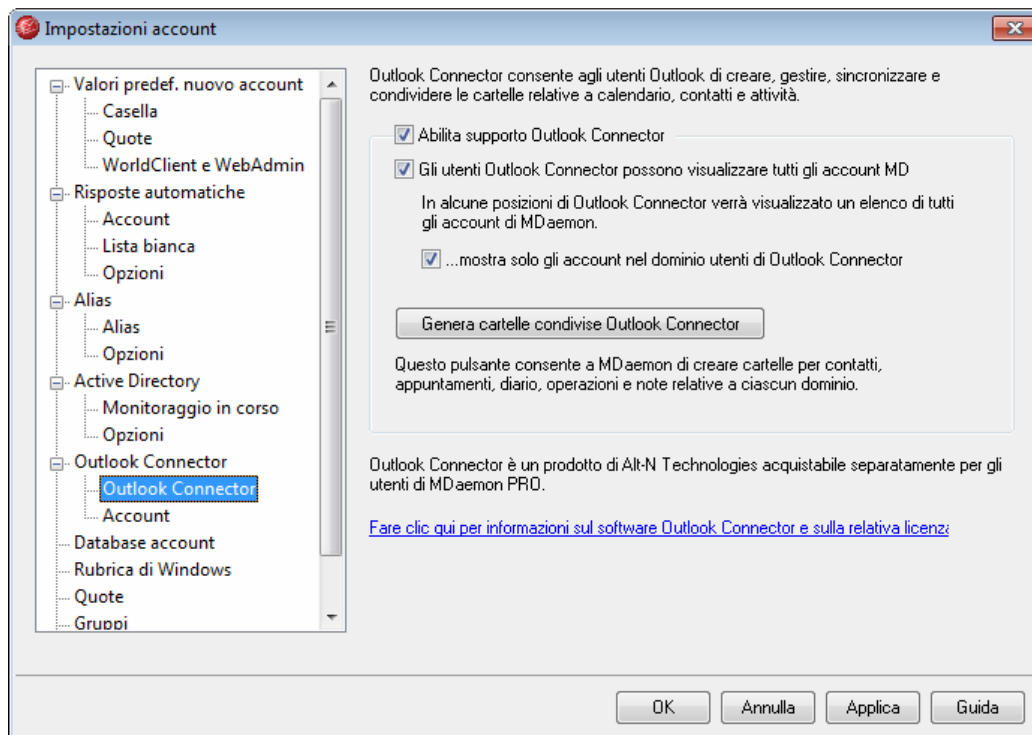
La versione più aggiornata di MDaemon PRO include il supporto di *MDaemon Outlook Connector*, un prodotto di Alt-N Technologies concesso in licenza separatamente. Outlook Connector consente di condividere con altri utenti il calendario, le informazioni sui contatti, le attività e altri elementi di Microsoft Outlook, senza richiedere Microsoft Exchange Server. MDaemon Outlook Connector è uno strumento efficace che consente di non utilizzare più Exchange.

Una volta installato Outlook Connector, la relativa finestra di dialogo sarà accessibile dalla barra dei menu di MDaemon, disponibile in: Account » Impostazioni account » Outlook Connector. Questa finestra può essere utilizzata per attivare e configurare Outlook Connector, nonché per consentirne l'uso a specifici account.

Per ulteriori informazioni o per scaricare Outlook Connector, visitare la pagina Outlook Connector per MDaemon del sito www.altn.com.

Vedere:

Opzioni Outlook Connector 406
Account di Outlook Connector 407

6.2.5.1 Opzioni di Outlook Connector

Outlook Connector

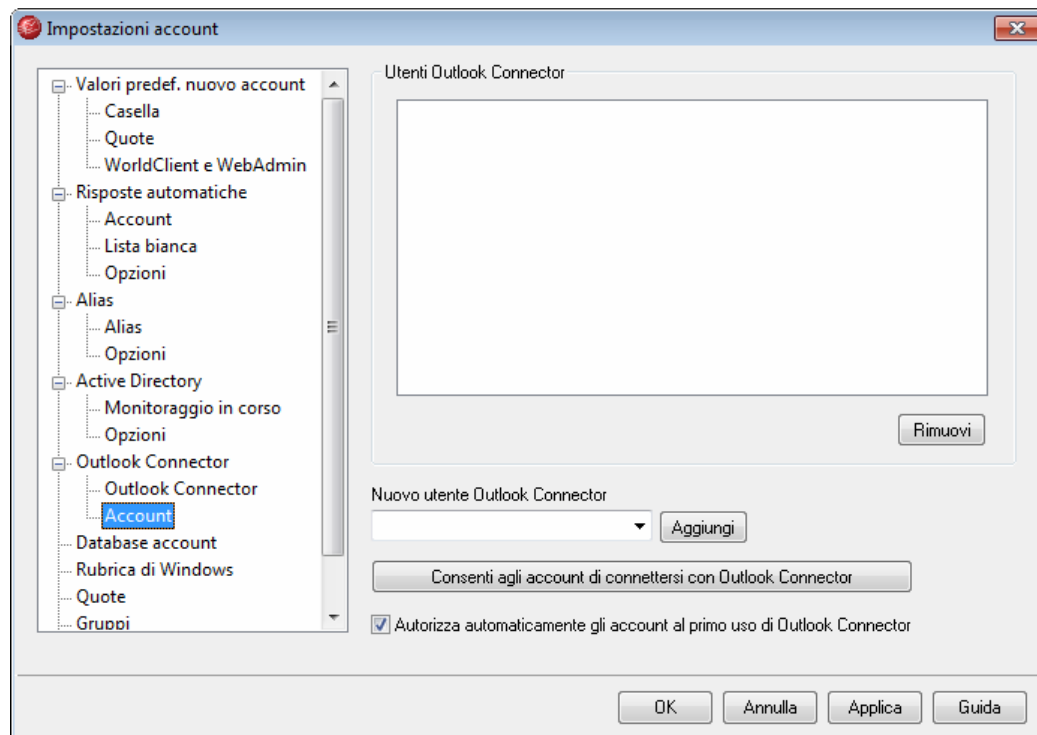
Abilita supporto Outlook Connector
Selezionare questa casella di controllo per attivare MDaemon Outlook Connector. Se non si seleziona questa opzione, gli utenti non potranno utilizzare le funzioni di Outlook Connector.

Gli utenti Outlook Connector possono visualizzare tutti gli account MD
Questa opzione consente la visualizzazione di tutti gli account di MDaemon, autorizzati per la connessione mediante Outlook Connector, nell'elenco *Autorizzazioni* che si trova nel plug-in di Outlook Connector per MDaemon. Gli utenti di Outlook Connector sceglieranno nell'elenco gli account ai quali desiderano concedere il diritto di condividere gli elementi di Outlook. Se si disabilita questa funzione, l'elenco *Autorizzazioni* del plug-in di Outlook Connector sarà vuoto e sarà necessario inserire gli indirizzi e-mail manualmente. In questo caso, potranno condividere gli elementi di Outlook solo gli indirizzi appartenenti agli account autorizzati per la connessione mediante Outlook Connector. Se un utente immette un indirizzo non autorizzato, quest'ultimo non potrà condividere gli elementi, a meno che non venga autorizzato a connettersi in un momento successivo.

...mostra solo gli account nel dominio utenti di Outlook Connector
Questa opzione è disponibile solo qualora sia stata abilitata l'opzione *Gli utenti Outlook Connector possono visualizzare tutti gli account MD*. Selezionare questa casella di controllo se si desidera visualizzare nell'elenco *Autorizzazioni* del plug-in di Outlook Connector solo gli utenti autorizzati a connettersi mediante Outlook Connector che appartengano allo stesso dominio. Gli account appartenenti a

domini diversi non verranno visualizzati, anche se autorizzati a connettersi mediante Outlook Connector.

Genera cartelle condivise Outlook Connector
Fare clic su questo pulsante per generare un insieme di cartelle di Outlook Connector per ogni dominio. Verranno create le cartelle dei contatti, degli appuntamenti, del diario, delle attività e delle note.

6.2.5.2 Account

Utenti Outlook Connector

In questo elenco vengono indicati gli utenti di MDaemon autorizzati a condividere le cartelle, il calendario, le note e le informazioni sui contatti di Outlook mediante Outlook Connector. Per aggiungere utenti all'elenco, utilizzare le opzioni descritte di seguito.

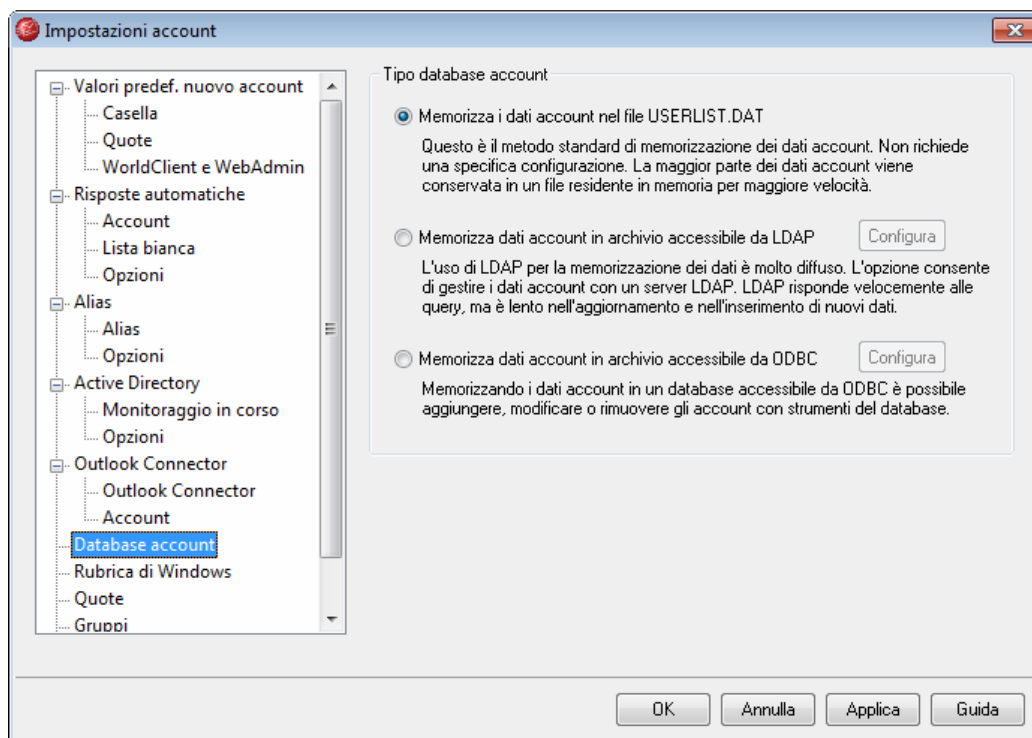
Nuovo utente Outlook Connector
Per aggiungere un utente di MDaemon all'elenco degli utenti autorizzati di Outlook Connector, selezionare la voce desiderata nell'elenco a discesa e fare clic su *Aggiungi* .

Aggiungi
Dopo aver selezionato un utente dall'elenco a discesa *Nuovo utente Outlook Connector*, fare clic su questo pulsante per aggiungere l'account all'elenco di utenti autorizzati di Outlook Connector.

Rimuovi
Per rimuovere una voce dall'elenco degli utenti autorizzati di Outlook Connector, selezionare l'elemento desiderato e fare clic su *Rimuovi*.

Consenti agli account di connettersi con Outlook Connector
Per autorizzare immediatamente tutti gli account MDaemon a connettersi mediante Outlook Connector, fare clic su questo pulsante. Tutti gli account verranno aggiunti all'elenco *Utenti Outlook Connector*.

Autorizza automaticamente gli account al primo uso di Outlook Connector
Selezionare questa casella di controllo se si desidera aggiungere automaticamente all'elenco *Utenti Outlook Connector* i singoli utenti al momento della prima connessione mediante Outlook Connector. **Nota:** se si attiva questa opzione, si autorizzano implicitamente all'uso di MDaemon Outlook Connector tutti gli account MDaemon. L'account non viene aggiunto all'elenco finché non viene utilizzato per la prima volta.

6.2.6 Database account

La finestra di dialogo Tipo database account, disponibile in Account » Impostazioni account , consente di indicare il metodo desiderato per la gestione degli account utente in MDaemon: ODBC, LDAP o il sistema `USERLIST.DAT` locale.

Memorizza i dati account nel file USERLIST.DAT
Selezionare questa opzione per abilitare l'uso del file interno `USERLIST.DAT` come

database dell'account. Questa è l'impostazione predefinita e consente di memorizzare a livello locale tutte le informazioni sugli account utente di MDaemon. La maggior parte delle informazioni viene memorizzata in un singolo file residente in memoria per aumentare efficienza e velocità.

Memorizza dati account in archivio accessibile da LDAP
Selezionare questa opzione se si desidera che MDaemon utilizzi il server LDAP come database utenti di MDaemon al posto di ODBC o del sistema `USERLIST.DAT` locale. Questo metodo di aggiornamento dei dati dell'account utente può risultare utile se si dispone di più server MDaemon in siti diversi che utilizzano un database utenti condiviso. Ciascun server MDaemon viene configurato per connettersi allo stesso server LDAP in modo da condividere le informazioni utente anziché salvarle a livello locale. Generalmente, i server LDAP rispondono in modo rapido ed efficiente alle query, ma sono più lenti nell'aggiornamento o nell'inserimento di nuovi dati.

Configura
Quando si seleziona l'opzione relativa a LDAP, questo pulsante consente di aprire la schermata LDAP101 per la configurazione delle impostazioni del server LDAP.

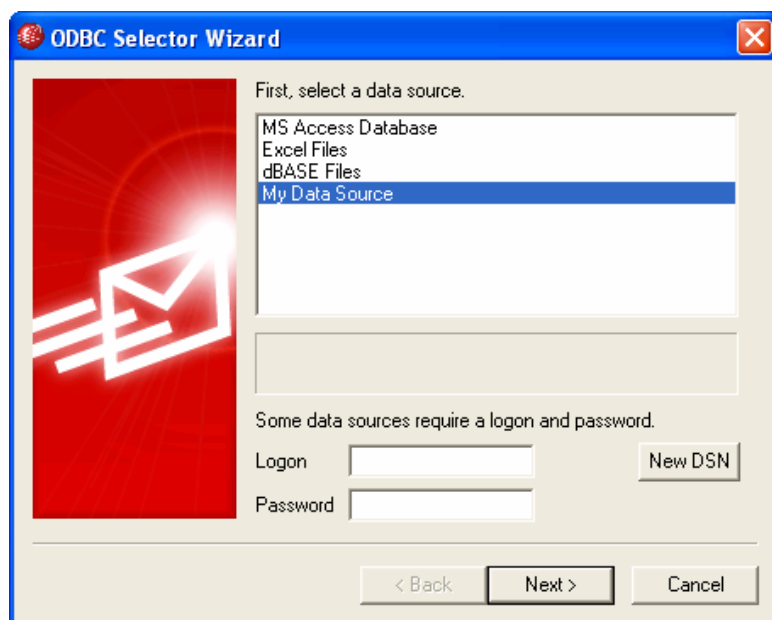
Memorizza dati account in archivio accessibile da ODBC
Questa opzione consente di utilizzare un database compatibile con ODBC per memorizzare i dati degli account di MDaemon.

Configura
Quando è specificata l'opzione relativa a ODBC, questo pulsante consente di attivare Selezione guidata ODBC409 al fine di selezionare e configurare il database compatibile ODBC.

6.2.6.1 Selezione guidata ODBC

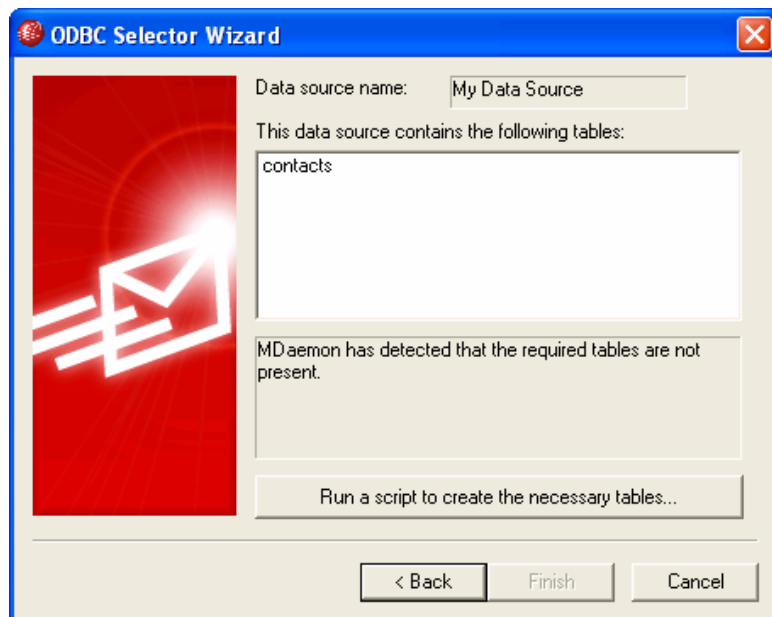
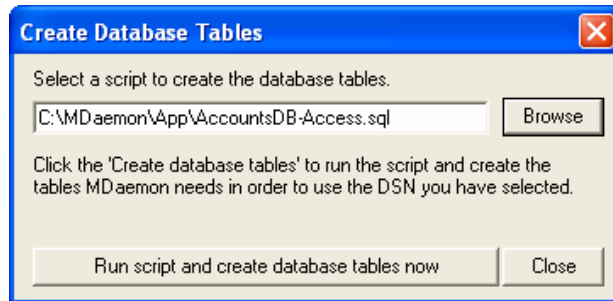
Selezione guidata ODBC consente di selezionare o configurare un'origine dati compatibile con ODBC da utilizzare come database degli account di MDaemon.

Migrazione del database utenti in un archivio accessibile da ODBC

1. Nella finestra di dialogo Opzioni database account (Account » Impostazioni account » Database account), fare clic su Memorizza dati account in archivio accessibile da ODBC, quindi su Configura per aprire Selezione guidata ODBC.

2. Selezionare l'origine dati desiderata per il database account. Se questa non è presente nell'elenco, fare clic su Nuovo DSN e seguire le indicazioni fornite in **Creazione di una nuova origine dati ODBC** 411.

3. Se necessario, inserire l'ID accesso e la Password dell'origine dati.

4. Scegliere Avanti.

5. Se l'origine dati include già le tabelle necessarie per MDaemon, proseguire con il **Passaggio 8.** In caso contrario, fare clic su Esegui script per creare le tabelle necessarie.

6. Inserire il percorso (o scegliere Sfoglia) del file di script da utilizzare per creare le tabelle dell'applicazione database. Nella cartella `\MDaemon\app\` sono presenti gli script per la maggior parte delle applicazioni database.

7. Scegliere Esegui script e crea tabelle del database, quindi OK e Chiudi.

8. Per chiudere la finestra di dialogo Opzioni del database dell'account, scegliere Fine e OK.

9. Lo strumento di migrazione del database trasferirà tutti gli account utente nell'origine dati ODBC e chiuderà MDaemon. Per iniziare a utilizzare il nuovo database utenti ODBC, scegliere OK e riavviare MDaemon.

Per ulteriori informazioni, vedere:

Database account 408
Creazione di una nuova origine dati ODBC 411

6.2.6.1.1 Creazione di una nuova origine dati

Per creare una nuova origine dati ODBC procedere come segue:

1. Nella finestra di dialogo Opzioni database account (Account » Impostazioni account » Database account), fare clic su Memorizza dati account in archivio accessibile da ODBC, quindi su Configura per aprire Selezione guidata ODBC.

2. Fare clic su Nuovo DSN per aprire la finestra di selezione dell'origine dati.

3. Passare alla scheda Origine dati computer e fare clic su Nuova per aprire la finestra di dialogo Crea nuova origine dati.

4. Selezionare Origine dati di sistema e fare clic su Avanti.

5. Selezionare il driver di database desiderato per l'origine dati, quindi fare clic su Avanti.

6. Fare clic su Fine per visualizzare la finestra di dialogo per l'impostazione dello specifico driver. L'aspetto di questa finestra di dialogo varia a seconda del driver selezionato. Quella visualizzata di seguito è la finestra di dialogo relativa alle impostazioni di accesso Microsoft.

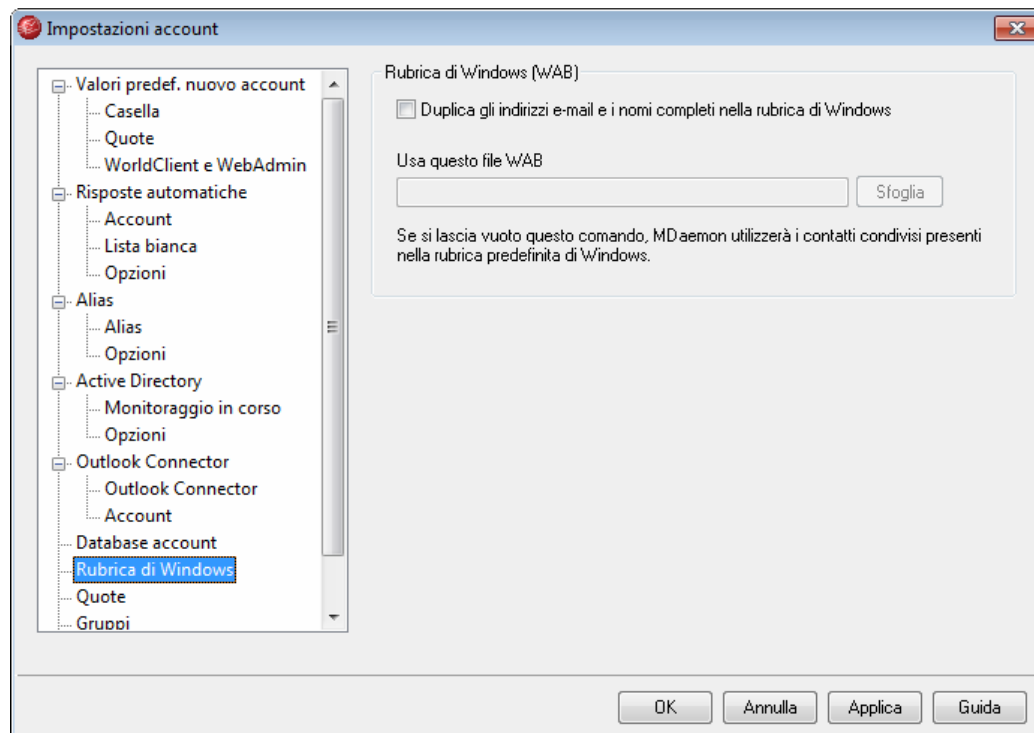
7. Indicare un valore per la nuova origine nel campo Nome origine dati e fornire le altre informazioni richieste dalla finestra di dialogo relativa allo specifico driver, quali la creazione o l'indicazione di un database, la scelta di una directory o di un server e così via.

8. Fare clic su OK per chiudere la finestra di dialogo del driver.

9. Fare clic su OK per chiudere la finestra di selezione dell'origine dati.

Vedere:

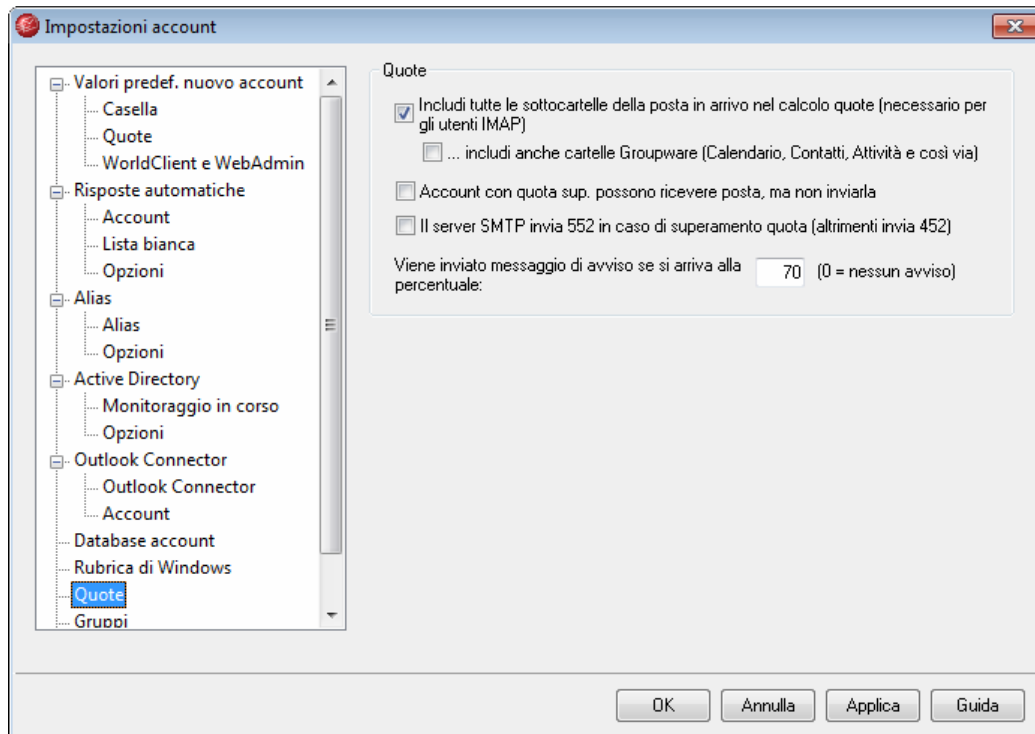
Database account 408
Selezione guidata ODBC - Database account 409

6.2.7 Rubrica di Windows

MDaemon è in grado di aggiornare automaticamente i nomi e gli indirizzi e-mail degli account presenti in un file della rubrica di Windows (*.wab) o nell'archivio dei contatti di Microsoft Outlook. Questa procedura è utile per condividere una rubrica con più utenti di prodotti come Outlook, senza che sia necessario utilizzare un server LDAP o ComAgent.

Rubrica di Windows (WAB)

Duplica gli indirizzi e-mail e i nomi completi nella rubrica di Windows
Selezionare questa casella di controllo per duplicare i nomi e gli indirizzi e-mail degli utenti in un file `*.wab` o nell'archivio dei contatti di Microsoft Outlook. È possibile configurare la rubrica di Windows per la condivisione delle informazioni dei contatti tra Outlook e le altre applicazioni. A tal fine, i dati possono essere memorizzati nell'archivio dei contatti di Microsoft Outlook o in un file di rubrica (con estensione `wab`). I comandi per questa operazione sono disponibili nel menu Strumenti→Opzioni della Rubrica di Windows.

Usa questo file WAB
Specificare il percorso del file con estensione `wab` in cui duplicare le informazioni sugli utenti. Se questo campo rimane vuoto, MDaemon utilizza l'archivio dei contatti condivisi della rubrica predefinita di Windows.

6.2.8 Quote

Quote

Includi tutte le sottocartelle della posta in arrivo nel calcolo delle quote (necessario per gli utenti IMAP)
Se questa casella di controllo è selezionata, i limiti di dimensione e quantità relativi ai messaggi impostati per la casella della posta in arrivo di un utente vengono applicati a tutti i file e a tutte le sottocartelle. Altrimenti, i limiti vengono applicati solo ai file messaggio veri e propri. Questo è generalmente necessario solo per gli utenti IMAP.

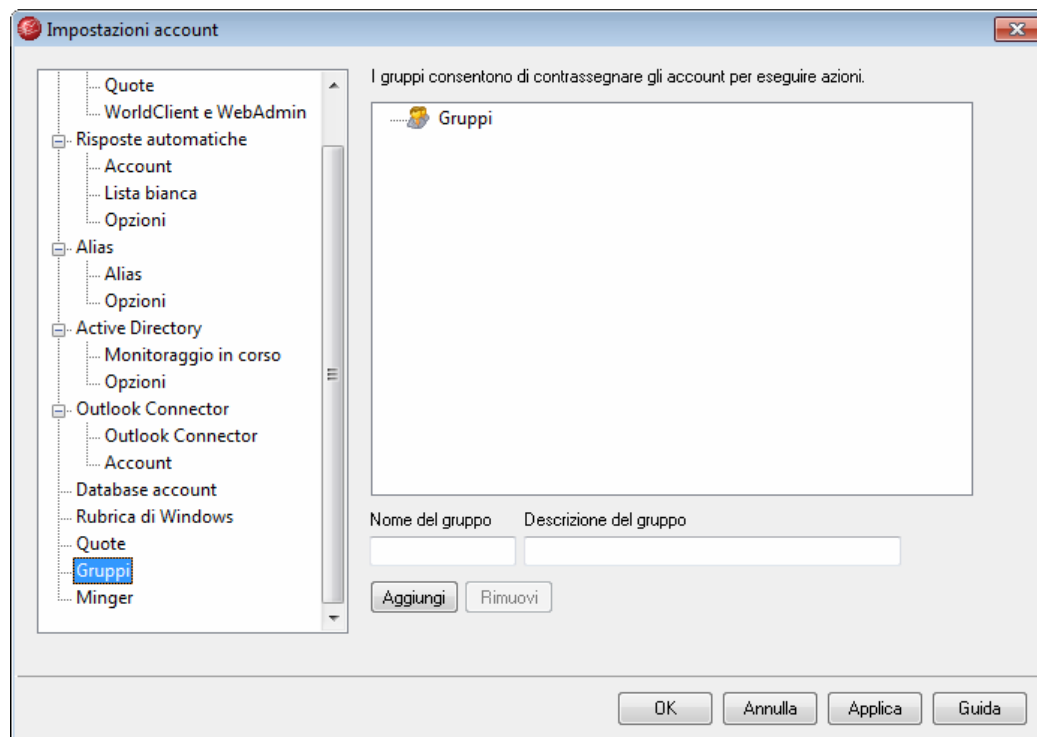
...includi anche cartelle Groupware (Calendario, Contatti, Attività e così via)
Selezionare questa casella di controllo se si desidera includere nel calcolo delle quote tutte le cartelle GroupWare, ad esempio calendari, contatti, attività e così via.

Account con quota sup. possono ricevere posta, ma non inviarla
Generalmente, se per un account è stato impostato un limite di quota, quando questo viene superato il titolare non può più ricevere messaggi. Finché non vengono eliminati alcuni messaggi, MDaemon non accetta posta per quell'account. Dopo aver superato la quota è ancora possibile, tuttavia, *inviare* messaggi. Specificare questa opzione se si desidera che tale restrizione venga gestita esattamente nel modo opposto, ovvero per indicare che l'account può *ricevere* ma non *inviare* posta dopo il superamento della quota.

Il server SMTP invia 552 in caso di superamento quota (altrimenti invia 452)
Per impostazione predefinita, quando un account supera la quota, MDaemon invia il

codice di errore 452 ("Azione richiesta respinta: spazio su sistema insufficiente") durante l'elaborazione SMTP. Questo codice indica generalmente che il server deve effettuare un tentativo successivo. Selezionando questa casella di controllo invece, viene inviato il codice di errore permanente 552 ("Azione richiesta interrotta: spazio dedicato superato").

Viene inviato messaggio di avviso se si arriva alla percentuale [xx] (0=nessun avviso)
Questo valore percentuale viene utilizzato per stabilire il valore della quota *Numero massimo di messaggi memorizzati contemporaneamente* o *Massimo spazio su disco consentito* definito in Account Editor 364 superato il quale verrà inviato un messaggio di avviso all'account. Nel messaggio verranno inclusi il numero di messaggi memorizzati e la dimensione della casella postale relativi all'account, nonché la percentuale utilizzata e la percentuale rimanente. Se nella casella postale dell'account è già presente un messaggio di avviso, questo viene sostituito dal messaggio aggiornato. Per disabilitare i messaggi di avviso, inserire il valore "0".

6.2.9 Gruppi

Gruppi

Questa finestra di dialogo consente di creare gruppi di account ai quali è possibile associare gli account utente. È possibile aggiungere membri ai gruppi utilizzando singole impostazioni account 345 e creare condizioni per le regole 214 di Filtro contenuti basate sull'appartenenza o meno a un gruppo specifico del mittente o del destinatario di un messaggio. È inoltre possibile assegnare a specifici gruppi i diritti ACL (Access Control List) 80 relativi alle cartelle condivise 75. Tali diritti verranno condivisi da tutti

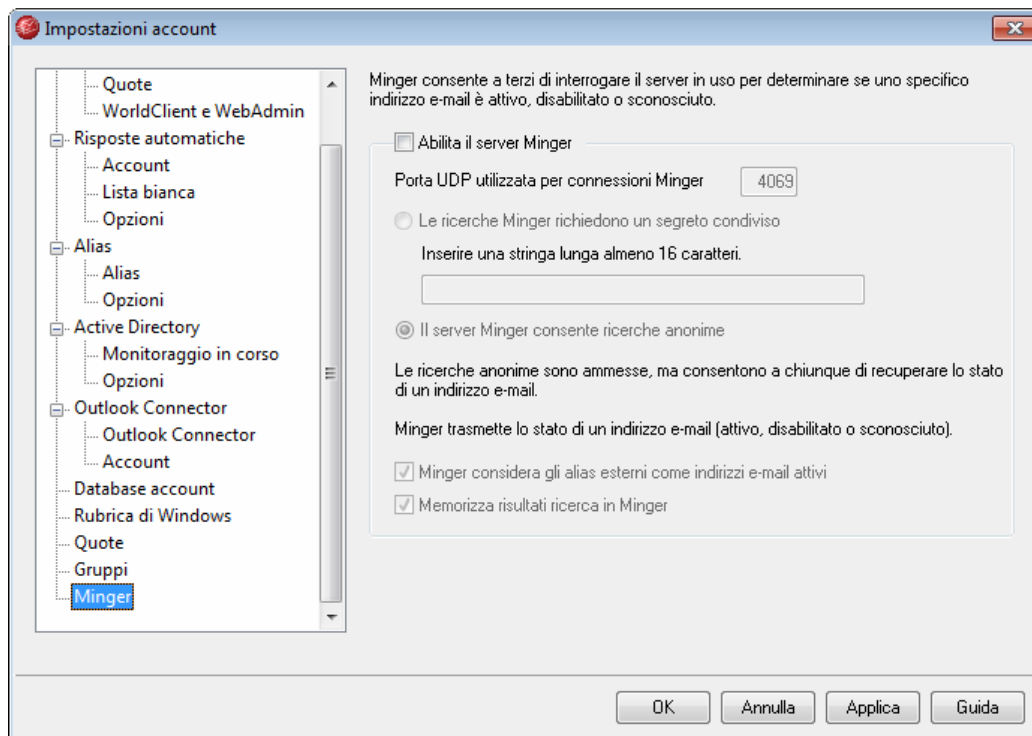
gli appartenenti al gruppo.

Nome del gruppo
Per creare un nuovo gruppo, digitarne il nome in questa casella, aggiungere una breve descrizione del gruppo in *Descrizione del gruppo* e scegliere *Aggiungi*.

Descrizione del gruppo
Questa casella di testo consente di inserire una breve descrizione relativa a un nuovo gruppo.

Aggiungi
Dopo aver assegnato il nome e la descrizione del gruppo, fare clic su questo pulsante per aggiungerlo all'elenco dei gruppi.

Rimuovi
Per rimuovere un gruppo, selezionarlo dall'elenco e fare clic su *Rimuovi*.

6.2.10 Minger

Minger è un protocollo di verifica degli indirizzi e-mail creato da Alt-N Technologies, le cui opzioni sono disponibili in Account » Impostazioni account. Ispirato in origine dal protocollo Finger, lo scopo principale di Minger è fornire un semplice ed efficiente meccanismo di interrogazione del server in uso per verificare la validità di un indirizzo e-mail. Minger utilizza il protocollo UDP anziché TCP per motivi di efficienza e, se lo si desidera, richiede l'autenticazione, sebbene supporti anche query anonime. La finestra

di dialogo Minger consente di attivare o disattivare il server Minger di MDaemon, di indicare la porta utilizzata (la porta predefinità è 4069) e di scegliere se richiedere l'autenticazione tramite un segreto condiviso oppure se consentire le query anonime.

In MDaemon è disponibile un client Minger, integrato nel sistema Gateway di dominio. Per ulteriori informazioni, vedere Verifica462. È possibile configurare l'uso di Minger per ogni dominio per il quale MDaemon agisce da server gateway o server di backup. Se si abilita Minger, MDaemon si connette al server remoto per verificare se i destinatari dei messaggi in entrata relativi a tale dominio siano validi. In tal modo, non è più necessario attenersi all'assunto che tutti i destinatari rappresentino indirizzi validi.

Per visualizzare l'ultima specifica relativa al protocollo Minger, visitare il sito:

http://tools.ietf.org/html/draft-hathcock-minger-05

Server Minger

Abilita il server Minger
Fare clic su questa casella di controllo per abilitare il server Minger di MDaemon.

Porta UDP utilizzata per connessioni Minger
Consente di specificare la porta monitorata dal server Minger per le connessioni. L'autorithy IANA (Internet Assigned Numbers Authority) ha riservato la porta TCP e UDP 4069 ai client e ai server Minger. Non è consigliabile modificare la porta utilizzata, perché è riservata esclusivamente a Minger.

Le ricerche Minger richiedono un segreto condiviso
Se si desidera richiedere l'autenticazione mediante un segreto condiviso, scegliere questa opzione e inserire una stringa di testo lunga almeno almeno 16 caratteri. Se si utilizza questa opzione, il server Minger respinge automaticamente le ricerche prive di autenticazione.

Il server Minger consente ricerche anonime
Selezionare questa opzione se si desidera che il server Minger consenta le ricerche anonime. In questo caso, al client che esegue la connessione non viene richiesto di eseguire l'autenticazione prima della ricerca. Il funzionamento di questa opzione è simile a quanto può essere realizzato utilizzando il comando `SMTP VRFY`, ossia la richiamata o l'inoltro di chiamata SMTP, ma è molto più efficiente e non provoca i problemi relativi a questi metodi, ossia la chiusura di numerose sessioni SMTP su TCP, l'affollamento dei file registro SMTP con le informazioni relative alle sessioni perse e così via.

Minger considera gli alias esterni come indirizzi e-mail attivi
Se si abilita questa casella, Minger considera gli alias esterni, ossia quelli che puntano a indirizzi esterni, come indirizzi attivi noti. Questa è la modalità operativa applicata anche alle interrogazioni eseguite da SecurityGateway in MDaemon, indipendentemente dall'impostazione di questa opzione.

Memorizza risultati ricerca Minger
Per impostazione predefinita, MDaemon memorizza nella cache i risultati della ricerca Minger. Se non si desidera che li memorizzi nella cache, disabilitare questa opzione.

6.3 Importazione degli account

6.3.1 Importazione degli account da un file di testo

Per accedere a questa funzione di generazione degli account, scegliere Account→ Importazione→Importa account da file di testo delimitato da virgole . La stessa funzione può essere attivata facendo clic sul pulsante *Importa* di Account Manager. Si tratta di un metodo semplice per importare e generare automaticamente gli account di posta. MDaemon legge il file di testo e genera i nuovi account utilizzando solo i nomi e i cognomi degli utenti. Se si impostano con attenzione le stringhe di modello per l'account corrette (vedere Valori predefiniti nuovo account 377), è possibile generare account univoci utilizzando solo i nomi e i cognomi degli utenti. Inoltre, se si desidera ignorare i valori predefiniti del nuovo account, è possibile includere numerose altre opzioni relative a impostazioni specifiche per l'utente. Tutti i campi devono essere separati da virgole.

Ogni riga del file di testo separato da virgole deve contenere una sola voce. La prima riga del file deve essere un'intestazione che fornisce i nomi e la sequenza dei campi delle righe successive. Di seguito è riportato un esempio di file corretto:

```
"Mailbox", "FullName", "MailDir", "AllowAccess"
"maurizio", "Maurizio Argento", "C:\Mail\Maurizio\", Y
"franco", "Franco Tommaso", "C:\Mail\Franco\", N
```

I nomi dei campi dell'intestazione vengono esaminati da MDaemon per determinare la sequenza dei dati e possono pertanto comparire in qualunque ordine. Ogni nome di campo deve essere racchiuso tra virgolette.

Tutti i valori di tipo stringa devono essere racchiusi tra virgolette e un valore di tipo "bool" (vero o falso) viene considerato `FALSE` a meno che il primo carattere sia: `y`, `Y`, `1`, `t` o `T`.

Per ogni nome completo vengono accettati il nome, il secondo nome e il cognome. Tuttavia, questi non possono essere separati da virgole.

Una volta eseguito il processo di importazione, MDaemon crea il file `TXIMPORT.LOG` che contiene i risultati dell'importazione, incluso un elenco degli account importati e non importati. In genere, non è possibile eseguire un'importazione perché vengono rilevati conflitti con la casella postale, il nome o le informazioni di directory di un account esistente, con l'alias esistente di un account oppure con il nome di una lista di

> distribuzione.
>
> Per ulteriori informazioni sulle corrispondenze tra campi, consultare la descrizione di `MD_ImportUserInfo()` e di `MD_ExportAllUsers()` nel file `MD-API.HTML` file, situato nella cartella `\API\`.

Per impostare la corrispondenza con i campi degli account di MDaemon, utilizzare nell'intestazione i valori seguenti:

Nome campo	Tipo
MailBox	stringa
Domain	string
FullName	string
MailDir	string
Password	string
AutoDecode	booleano
IsForwarding	bool
AllowAccess	bool
AllowChangeViaEmail	bool
KeepForwardedMail	bool
HideFromEveryone	bool
EncryptMail	bool
ApplyQuotas	bool
EnableMultiPOP	bool
MaxMessageCount	intero
MaxDiskSpace	int
FwdAddress	string
FwdHost	string
FwdSendAs	string
FwdPort	string
NTAccount	string
MailFormat	string
AutoRespScript	string
AutoRespProcess	string
AddToList	string
RemoveFromList	string

PassMessageToProcess	bool
MaxUIDLCount	int
MaxMessageSize	int
RecurseIMAP	bool
MaxInactive	int
MaxMessageAge	int
MaxDeletedIMAPMessageAge	int
Comments	string
UserDefined	stringa

Per ulteriori informazioni, vedere

Integrazione con gli account Windows 422

6.3.2 Integrazione con gli account Windows

MDaemon supporta l'integrazione con gli account Windows. Tale supporto consiste in un modulo di importazione da SAM/Active Directory, al quale è possibile accedere selezionando Account→Importazione→Importa account da SAM/Active directory. Inoltre, nel software di gestione utenti di MDaemon è incorporato il supporto per l'autenticazione dinamica degli utenti. È possibile specificare un dominio Windows nel campo della password di un account in modo che MDaemon autentichi dinamicamente e in tempo reale tale account mediante il sistema di protezione del dominio Windows specificato. Se è in uso uno schema di questo tipo, la modifica della password dell'account nella Gestione utenti di Windows aggiorna automaticamente MDaemon. Di conseguenza, gli utenti devono ricordare solo un set di credenziali di autenticazione. Ciò consente inoltre di semplificare la configurazione delle nuove installazioni.

Il contesto di protezione dell'account che esegue MDaemon deve includere il privilegio **SE_TCB_NAME** (ossia Agisci come parte del sistema operativo). Se è un servizio in esecuzione nell'account *Local System*, il processo dispone di questo privilegio per impostazione predefinita. In caso contrario, è necessario impostare nella gestione utenti di Windows tale privilegio per l'account in cui MDaemon è in esecuzione.

Funzione di importazione degli account di SAM/Active Directory

Domini

Nome computer PDC/BDC
In questo campo è possibile specificare il nome del sistema da cui MDaemon legge le informazioni sul database degli account Windows. Specificando \\<DEFAULT>, MDaemon leggerà i dati dal sistema locale.

Aggiorna
Fare clic su questo pulsante per aggiornare l'elenco degli account Windows.

Nome dominio di Windows
Digitare il nome dominio Windows da cui si desidera importare gli account.

Nome dominio MDaemon
Selezionare dalla casella di riepilogo a discesa il dominio MDaemon in cui importare gli account.

Account

Account di Windows
In questa finestra viene fornito un elenco di tutti i nomi di account raccolti dal database degli account Windows.

Account
In questa finestra vengono riportati tutti i nomi degli account selezionati per l'importazione.

>>
Fare clic su questo pulsante per spostare i nomi account evidenziati dalla finestra "Account di Windows" alla finestra "Account selezionati".

<<
Fare clic su questo pulsante per rimuovere le voci evidenziate dalla finestra "Account selezionati".

Opzioni

Usa nomi di account di SAM/AD per le caselle postali degli account
Selezionare questa casella di controllo per utilizzare il nome dell'account Windows di ciascun utente come valore della relativa casella postale. In questo modo, non è necessario configurare apposite macro per il modello dei nuovi account377.

Usa modelli di account per generare le password
Se si seleziona questa opzione, MDaemon genererà le password per gli account importati utilizzando le impostazioni del modello di account. Al riguardo, vedere Valori predefiniti account377.

Imposta pwd account = ai nomi di account
Se si seleziona questa casella di controllo, MDaemon utilizzerà il nome dell'account come password per l'account.

Rendi tutte le password uguali a
Questa opzione consente di specificare un valore di password statico che verrà utilizzato da tutti gli account importati.

Autentica le password dinamicamente con SAM/AD
Se si seleziona questa casella di controllo, gli account importati verranno autenticati dinamicamente. Anziché specificare una password, MDaemon autenticherà in tempo reale i valori USER e PASS forniti dal client di posta mediante il database di NT.

Autentica su questo dominio Windows
Immettere il nome dominio di Windows utilizzato da MDaemon durante l'autenticazione dinamica delle connessioni. **Questo non è il nome computer del controller del dominio, ma il nome effettivo del dominio Windows.**

Quando gli account sono configurati per l'autenticazione dinamica, il nome del dominio Windows (preceduto da due caratteri di barra rovesciata) viene utilizzato nel campo `PASSWORD` dell'account e viene memorizzato in formato non crittografato nel file `USERLIST.DAT`. Ad esempio, se un account è configurato per l'autenticazione dinamica su un dominio Windows di nome `ALTN`, il campo relativo alla password

dell'account contiene il valore \\ALTN. I due caratteri di barra rovesciata che precedono il nome del dominio indicano a MDaemon che il campo relativo alla password contiene effettivamente il nome di un dominio Windows. MDaemon deve quindi tentare di utilizzare il database degli account del dominio per l'autenticazione dei valori USER e PASS forniti dal client di posta. Per questo motivo, è necessario non inserire password precedute da due barre rovesciate a meno che l'account non sia stato configurato per l'autenticazione dinamica nel modo appena descritto. In altri termini, le password normali non possono iniziare con due barre rovesciate. Di regola, si presuppone che questo tipo di password rappresenti un nome di un dominio Windows e non una password.

È possibile inserire una combinazione di due caratteri di barra rovesciata e del nome dominio Windows nel campo relativo alla password dell'account nella scheda Account 343 di Account Editor. Per configurare gli account per l'autenticazione dinamica non è indispensabile utilizzare la funzione di importazione..

Vedere:

Importazione degli account da un file di testo 420

Account Editor » Account 343

Sezione VII

7 Menu Liste

7.1 Liste di distribuzione

Le liste di distribuzione (definite anche "mailing list") consentono di inviare messaggi a gruppi di utenti, come se questi condividessero la stessa casella postale. Le copie dei messaggi e-mail inviati alla lista vengono distribuite a ciascun iscritto dellalista. Le liste possono contenere membri con indirizzi di destinazione locale e/o remota, possono essere pubbliche o private, moderate o aperte, possono venire inviate in formato riassunto o normale e così via.

Editor delle liste di distribuzione

L'editor delle liste di distribuzione, disponibile in Liste » Nuova lista di distribuzione o Liste » Modifica lista di distribuzione, consente di creare e gestire liste di distribuzione. Sono disponibili le schermate seguenti:

Impostazioni 429
Membri 431
Iscrizione 434
Moderazione 438
Impostazioni riassunto 439
Instradamento 441
Notifiche 442
File supporto 444
Cartella pubblica 445
Active Directory 446
ODBC 448

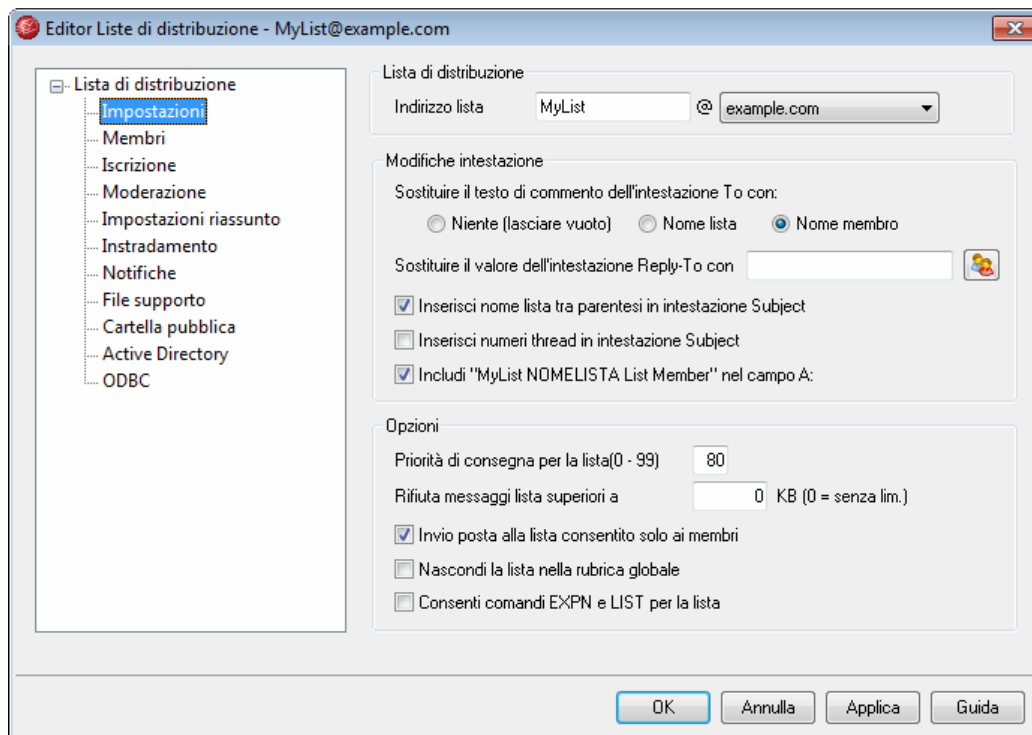
Creazione di una nuova lista di distribuzione

Selezionando Liste » Nuova lista...verrà visualizzata la finestra dell'editor delle liste di distribuzione, nella quale è possibile creare una nuova lista. Per creare una lista è sufficiente assegnarvi un nome e designarne il dominio di appartenenza. Tutte le altre opzioni contengono impostazioni predefinite. È possibile modificare queste impostazioni durante la creazione della lista oppure in un secondo momento.

Modifica di una lista di distribuzione esistente

Scegliere Liste » Modifica lista... per visualizzare la finestra di dialogo di selezione della lista di distribuzione. Quando è selezionata in questa finestra di dialogo, la lista viene aperta nell'editor delle liste di distribuzione per poter essere modificata o analizzata.

7.1.1 Editor delle liste di distribuzione

7.1.1.1 Impostazioni

Lista di distribuzione

Indirizzo lista
Specificare un nome per la lista di distribuzione, quindi scegliere il dominio di appartenenza dalla casella di riepilogo a discesa. I messaggi indirizzati a questa lista utilizzeranno il nome e il dominio specificato in questo campo, ad esempio `nomelista@nomedominio.com`. I nomi di lista non possono contenere i simboli "!" o "|".

Modifiche intestazione

Sostituire il testo di commento dell'intestazione 'TO:' con:
Questa opzione consente di indicare il testo da visualizzare nella parte relativa al commento, ossia al nome reale, dell'intestazione TO: quando MDaemon riceve un messaggio diretto alla lista.

Niente (lasciare vuota): selezionando questa opzione, MDaemon non apporta modifiche all'indirizzo visualizzato. L'indirizzo presente nell'intestazione TO: viene visualizzato nella forma in cui è stato inserito dal mittente.

Nome lista: con questa opzione, nell'intestazione TO: viene visualizzato l'indirizzo della lista di distribuzione.

Nome membro: con questa opzione, nell'intestazione TO: viene visualizzato il nome, se disponibile, e l'indirizzo dell'iscritto al quale è destinato il messaggio.

L'opzione *Nome membro* può essere selezionata solo se è stata selezionata l'opzione "*Consegna singolarmente posta lista a ciascun membro*" della schermata Instradamento441. Quando si seleziona "*Consegna posta lista tramite singoli comandi RCPT per ogni membro*", MDaemon utilizzerà per impostazione predefinita l'opzione relativa al *nome lista*.

Sostituire il valore dell'intestazione 'Reply-To' con
Digitare l'indirizzo e-mail a cui si desidera vengano indirizzate le risposte inviate a questa lista oppure selezionare l'icona Account per individuare l'account al quale inviare le risposte. Utilizzare l'indirizzo della lista se si desidera che le risposte vengano reindirizzate alla lista stessa. Se si lascia questo campo vuoto, le risposte a un messaggio inviato alla lista verranno rispedite al mittente del messaggio. In genere, le risposte ai messaggi di una lista di distribuzione vengono reindirizzate alla lista, anziché al mittente del messaggio.

Inserisci nome lista tra parentesi in intestazione Subject
Mediante questa impostazione, MDaemon racchiude il nome della lista tra parentesi (ad esempio, [Nomelista]) e lo aggiunge all'inizio dell'`oggetto` di tutti i messaggi inviati alla lista.

Inserisci numeri thread in intestazione Subject
Questa casella di controllo consente di specificare se visualizzare i numeri di thread nell'intestazione `Subject:` dei messaggi della lista. I numeri vengono apposti tra parentesi alla fine della riga dell'oggetto e utilizzati come numeri di pseudo-thread. Se si ordina la casella della posta in arrivo in base all'oggetto, i messaggi verranno disposti cronologicamente.

Includi "[nome lista] List Member" nel campo TO:
Quando si abilita questa funzione, nella porzione "nome reale" del campo TO: del messaggio viene visualizzato il nome della lista seguito da "List Member". Ad esempio, "`lista-franco List Member`".

Non tutti i client e-mail supportano la visualizzazione dei "nomi reali" nel campo TO: dei messaggi. In questi casi, viene visualizzato solo l'indirizzo e-mail effettivo specificato nell'opzione "*Sostituisci testo intestazione 'To:' con:*".

Opzioni

Priorità di consegna per la lista(0 - 99)
Inserire un numero compreso tra 0 e 99. Il valore indica l'ordinamento relativo dei messaggi durante il processo di consegna. Il valore è inversamente proporzionale all'importanza del messaggio e alla relativa posizione nell'ordine della coda dei messaggi. Di seguito viene fornita un'indicazione generica per l'assegnazione dei valori: 10 = Urgente, 50 = Normale e 80 = Collettivo.

Rifiuta messaggi lista superiori a XX KB
Questo comando pone un limite massimo alla dimensione dei messaggi accettati dalla lista di distribuzione. I messaggi che superano questo limite verranno rifiutati.

Invio posta alla lista consentito solo ai membri
Quando si abilita questo controllo, la lista viene considerata "privata" e solo gli iscritti possono inviare messaggi. I messaggi provenienti da utenti non iscritti alla lista vengono eliminati.

Nascondi la lista nella rubrica globale
Se si abilita questa opzione, la lista di distribuzione viene nascosta nelle rubriche pubbliche di WorldClient e di LDAP.

Consenti comandi EXPN e LIST per la lista
Se questa opzione è abilitata, l'appartenenza alla lista viene riportata in risposta al comando EXPN o LISTS durante una sessione di posta. Se l'opzione non è selezionata, l'appartenenza alla lista rimane privata.

7.1.1.2 Membri

Appartenenza

In questa casella vengono visualizzati gli indirizzi e-mail e i nomi di tutti coloro che sono attualmente iscritti alla lista. Per ogni appartenente viene indicato anche il tipo

di iscrizione: Normale, Riassunto, Solo lettura, Solo invio.

Rimuovi
Per rimuovere un iscritto dall'elenco, selezionare la voce desiderata e fare clic su questo pulsante.

Attivazione/disattivazione riassunto
Selezionare un iscritto, quindi fare clic su questo pulsante per designarlo come iscritto di tipo Riassunto439.

Attivazione/disattivazione sola lettura
Selezionare un iscritto e fare clic su questo pulsante per assegnargli lo stato "Sola lettura". L'utente continuerà a ricevere i messaggi dalla lista, ma non sarà in grado di inviarne.

Solo invio/no posta
Selezionare un iscritto e fare clic su questo pulsante per designarlo come iscritto di tipo "Solo invio". Con questo tipo di appartenenza, è possibile inviare messaggi alla lista, ma non riceverne.

Aggiunta di nuovi iscritti alla lista

E-mail nuovo membro
Inserire l'indirizzo e-mail dell'utente che si desidera aggiungere alla lista di distribuzione o fare clic sull'icona Account per individuare l'account MDaemon desiderato. Gli indirizzi dei membri della lista non possono contenere i simboli "!" e "|".

Per fare riferimento a tutti gli utenti di MDaemon o a tutti gli utenti di uno dei domini anziché a uno specifico indirizzo di posta elettronica, è possibile immettere rispettivamente `ALL_USERS` o `ALL_USERS:<dominio>`. Ad esempio, l'aggiunta di `ALL_USERS:esempio.com` come membro di una lista equivale ad aggiungere separatamente tutti gli account utente di `esempio.com`. L'aggiunta di `ALL_USERS` come membro della lista equivale ad aggiungere tutti gli account di MDaemon, indipendentemente dal dominio.

Nome reale
Inserire in questo campo il nome reale dell'iscritto. Il nome viene visualizzato nell'intestazione "To:" dei messaggi della lista se l'opzione "*Sostituisci intestazione 'To:' con nome membro*" in Impostazioni429 è selezionata.

Normale, Riassunto, Solo lettura, Solo invio
Fare clic sull'opzione che si desidera applicare all'indirizzo e-mail del *nuovo iscritto*.

Aggiungi
Questo pulsante consente di aggiungere all'elenco degli iscritti la voce contenuta nel campo *E-mail nuovo membro*.

Predefinito
Fare clic su una delle opzioni situate situate accanto a questo pulsante, *Normale, Riassunto, Solo lettura, Solo invio* e fare clic sul pulsante per designare tale opzione come predefinita per i nuovi iscritti.

Importa
Per importare gli iscritti alla lista di distribuzione da un file di testo con campi separati (delimitati) da virgole, scegliere questo pulsante. È necessario che esista una voce per ogni riga e che i campi siano delimitati da virgole. Nella prima riga del file, inoltre, deve essere riportato l'elenco dei campi e indicato l'ordine in cui questi vengono visualizzati nelle righe successive. Uno dei campi deve essere denominato "**`Email`**" e contenere gli indirizzi e-mail mentre, facoltativamente, può esisterne un altro denominato "**`FullName`**" con i nomi degli iscritti alla lista. Gli altri campi vengono ignorati dal programma di importazione.

Ad esempio:

```
"Email", "FullName", "Address", "telephone"
"franco@altn.com", "Franco Tommaso", "Via indipendenza 123",
"817.555.1234"
```

Gli iscritti importati non ricevono il messaggio di benvenuto alla lista, se previsto, e il programma di importazione non esegue controlli per l'eventuale duplicazione degli iscritti.

Rimuovi aut. gli indirizzi inattivi da lista membri
Quando questa funzione è abilitata e si verifica un errore irreversibile permanente durante una consegna, MDaemon rimuove automaticamente il relativo indirizzo dall'elenco degli iscritti. Gli indirizzi sono considerati inattivi e vengono rimossi anche quando il relativo messaggio viene spostato nella coda tentativi e, successivamente, viene considerato scaduto da tale coda.

L'opzione *Rimuovi automaticamente gli indirizzi inattivi...* è ideata esclusivamente allo scopo di offrire assistenza nei casi in cui il server di posta rifiuti di accettare i messaggi. Questa opzione è operativa solo quando viene selezionata l'opzione "*Consegna singolarmente posta lista a ciascun membro*" nella schermata Instradamento441. Se si instradano i messaggi della lista a un host intelligente, per ulteriori informazioni consultare *Sfoltimento avanzato della lista*.

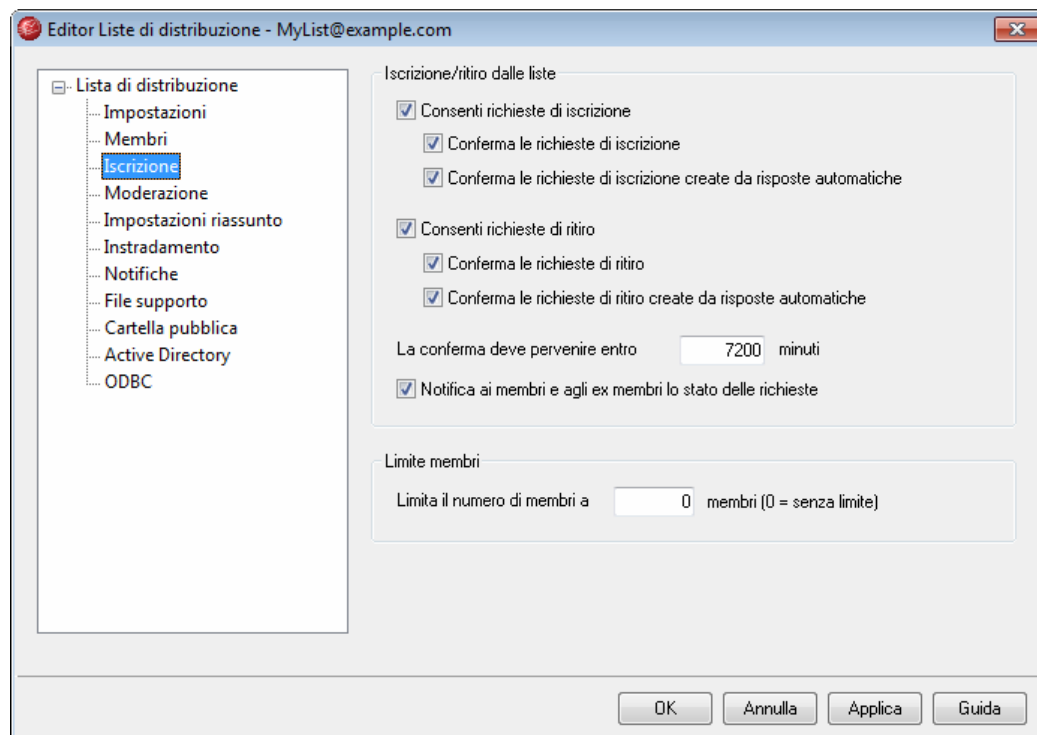
Numero di membri della lista:
Nella parte inferiore della schermata viene visualizzato il numero totale degli iscritti attualmente alla lista.

Sfoltimento avanzato della lista

Quando si abilita l'opzione *Rimuovi automaticamente gli indirizzi inattivi...* e come percorso di ritorno per i messaggi della lista viene specificata una casella postale locale (vedere l'opzione *Indirizzo di rispedizione SMTP dell'elenco* di Notifiche442), ogni giorno a

mezzanotte MDaemon tenta un'analisi degli indirizzi problematici della posta respinta e rimuove i membri che non è stato possibile raggiungere. In questo modo si sfoltiranno efficacemente gli indirizzi non validi delle liste di distribuzione, in particolare se si instradano i messaggi della lista a un host intelligente anziché consegnarli direttamente.

In Preferenze » Varie 202 esistono due opzioni relative a questa funzione. L'opzione *Lo sfoltimento elimina i msg non contenenti indirizzi analizzabili* determina l'eliminazione dei messaggi restituiti che non contengono indirizzi analizzabili, mentre l'opzione *Lo sfoltimento salva i msg per la rimozione dei membri lista* determina il salvataggio di tutti i messaggi associati a iscritti eliminati dalla lista.

7.1.1.3 Iscrizione

Iscrizione/ritiro dalle liste

Consenti richieste di iscrizione
Questa opzione determina se la lista consente richieste di iscrizione mediante messaggi e-mail appositamente formattati oppure mediante messaggi di risposta

automatica. Per ulteriori informazioni, vedere: Iscrizione alle liste di distribuzione 436.

Conferma le richieste di iscrizione
Quando si abilita questa casella di controllo, MDaemon tenta di confermare le richieste di iscrizione generando un codice univoco che viene incluso in un messaggio inviato all'indirizzo che ha richiesto di unirsi alla lista. Se la persona risponde al messaggio di conferma, MDaemon aggiunge automaticamente il membro alla lista. I messaggi di conferma hanno validità temporale limitata, ossia è necessario che la risposta dell'utente al messaggio venga ricevuta entro il numero di minuti indicato successivamente.

Conferma le richieste di ritiro create da risposte automatiche
Quando si abilita questa casella di controllo, MDaemon tenta di confermare le richieste di iscrizione generate automaticamente tramite l'opzione di risposta automatica 357 "*Aggiungi mittente a lista distribuzione*." Analogamente a quanto avviene con l'opzione precedente, MDaemon genera un codice univoco e lo include in un messaggio inviato all'indirizzo in attesa di essere aggiunto alla lista. Se la persona risponde al messaggio di conferma, MDaemon aggiunge automaticamente il membro alla lista. Anche questi messaggi di conferma hanno validità temporale limitata, pertanto richiedono una risposta entro il numero di minuti indicato successivamente.

Ritiro dell'iscrizione

Consenti richieste di ritiro
Questa opzione determina se la lista consente richieste di ritiro mediante messaggi e-mail appositamente formattati oppure mediante messaggi di risposta automatica. Per ulteriori informazioni, vedere: Iscrizione alle liste di distribuzione 436.

Conferma le richieste di ritiro
Quando si abilita questa casella di controllo, MDaemon tenta di confermare le richieste di ritiro di un membro dalla lista, generando un codice univoco che viene incluso in un messaggio inviato all'indirizzo che ha richiesto di annullare l'iscrizione alla lista. Se la persona risponde al messaggio di conferma, MDaemon ritira automaticamente il membro dalla lista. I messaggi di conferma hanno validità temporale limitata, ossia è necessario che la risposta dell'utente al messaggio venga ricevuta entro il numero di minuti indicato successivamente.

Conferma le richieste di ritiro create da risposte automatiche
Quando si abilita questa casella di controllo, MDaemon tenta di confermare le richieste di ritiro generate automaticamente tramite l'opzione di risposta automatica 357 "*Rimuovi mittente da lista distribuzione*." Analogamente a quanto avviene con l'opzione *Conferma le richieste di ritiro*, MDaemon genera un codice univoco e lo include in un messaggio inviato all'indirizzo in attesa di essere rimosso dalla lista. Se la persona risponde al messaggio di conferma, MDaemon rimuove automaticamente il membro. Anche questi messaggi di conferma hanno validità temporale limitata, pertanto richiedono una risposta entro il numero di minuti indicato successivamente.

La conferma deve pervenire entro XX minuti
Questo valore indica il numero di minuti disponibili prima della scadenza del

messaggio di conferma di iscrizione o di ritiro. Se questo limite viene superato prima che MDaemon riceva il messaggio di risposta, l'indirizzo non viene aggiunto o rimosso dalla lista. È necessario, quindi, che l'utente invii nuovamente la richiesta di iscrizione o di ritiro dalla lista. L'impostazione predefinita per questa opzione è di 7200 minuti, ossia cinque giorni.

Si tratta di un valore globale applicato a tutte le liste di distribuzione, non solo alla lista in corso di modifica.

Notifica ai membri e agli ex membri lo stato delle richieste
Quando questa opzione è abilitata, MDaemon invia un messaggio che notifica il completamento dell'operazione all'utente che si è iscritto/ritirato dalla lista di distribuzione.

Limite membri

Limita il numero di membri a [xx] membri (0 = senza limite))
Questa funzione consente di definire il numero massimo di persone autorizzate a iscriversi alla lista di distribuzione. Se non si desidera specificare alcun limite, immettere il valore zero.

Tale limite viene applicato solo agli indirizzi che si sono iscritti mediante i metodi e-mail descritti in *Iscrizione alle liste di distribuzione* 436. Non viene applicato, invece, agli iscritti inseriti manualmente nella schermata Membri 431, né alle richieste di iscrizione pervenute tramite e-mail nel caso esista una Password elenco 438.

Vedere:

Iscrizione alle liste di distribuzione 436
Risposte automatiche 357

7.1.1.3.1 Iscrizione alle liste di distribuzione

Iscrizione/ritiro mediante comandi e-mail

Per iscriversi o ritirarsi da una lista di distribuzione, inviare un messaggio e-mail indirizzato a `MDaemon` o a un suo alias appropriato presso il dominio che effettua l'hosting della lista di distribuzione e inserire il comando `Subscribe` o `Unsubscribe` come prima riga del corpo del messaggio. Ad esempio, se la lista di distribuzione `MD-Support` appartiene al dominio `altn.com`, è possibile iscriversi a essa componendo un messaggio indirizzato a "`mdaemon@altn.com`" in cui sia inserito il valore: `SUBSCRIBE MD-Support@altn.com` nella prima riga del corpo del messaggio. L'oggetto del messaggio è irrilevante e può essere lasciato vuoto.

Per informazioni più esaurienti su questo e altri messaggi di comando, vedere: Controllo remoto del server via e-mail506.

Talvolta gli utenti tentano di iscriversi o ritirarsi dalle liste via e-mail inviando i comandi alla lista stessa anziché all'account del sistema MDaemon. A seguito di questa azione, il comando viene inviato alla lista anziché all'utente che sta tentando di iscriversi o ritirarsi. Per prevenire la registrazione di tali messaggi nelle liste di distribuzione, esiste un'opzione situata in Impostazioni » Preferenze » Sistema194, denominata "*Cerca contenuto non pertinente nella posta delle liste di distribuzione*." L'opzione è abilitata per impostazione predefinita.

Iscrizione/ritiro mediante indirizzi e-mail

L'opzione "*Consenti gli indirizzi '<Lista>-subscribe' e '<Lista>-unsubscribe'*," situata in Impostazioni » Preferenze » Varie202 consente agli utenti di iscriversi o ritirarsi dalle liste di distribuzione inviando un messaggio a un determinato indirizzo e-mail, invece di utilizzare i comandi e-mail descritti precedentemente in *Iscrizione/ritiro mediante comandi e-mail*. Per iscriversi o ritirarsi da una lista utilizzando questo metodo, è sufficiente inviare un messaggio all'indirizzo della lista, aggiungendo "`-subscribe`" o "`-unsubscribe`" alla parte dell'indirizzo relativa alla casella postale. Se, ad esempio, il nome della lista è "`franco-lista@esempio.com`," è possibile iscriversi alla lista inviando un messaggio a "`franco-lista-subscribe@esempio.com`." Per ritirarsi, inviare il messaggio a "`franco-lista-unsubscribe@esempio.com`." In entrambi i casi, il contenuto dell'oggetto e del corpo del messaggio è irrilevante. Inoltre, quando questa funzione è attiva, MDaemon inserisce in tutti i messaggi della lista l'intestazione seguente:

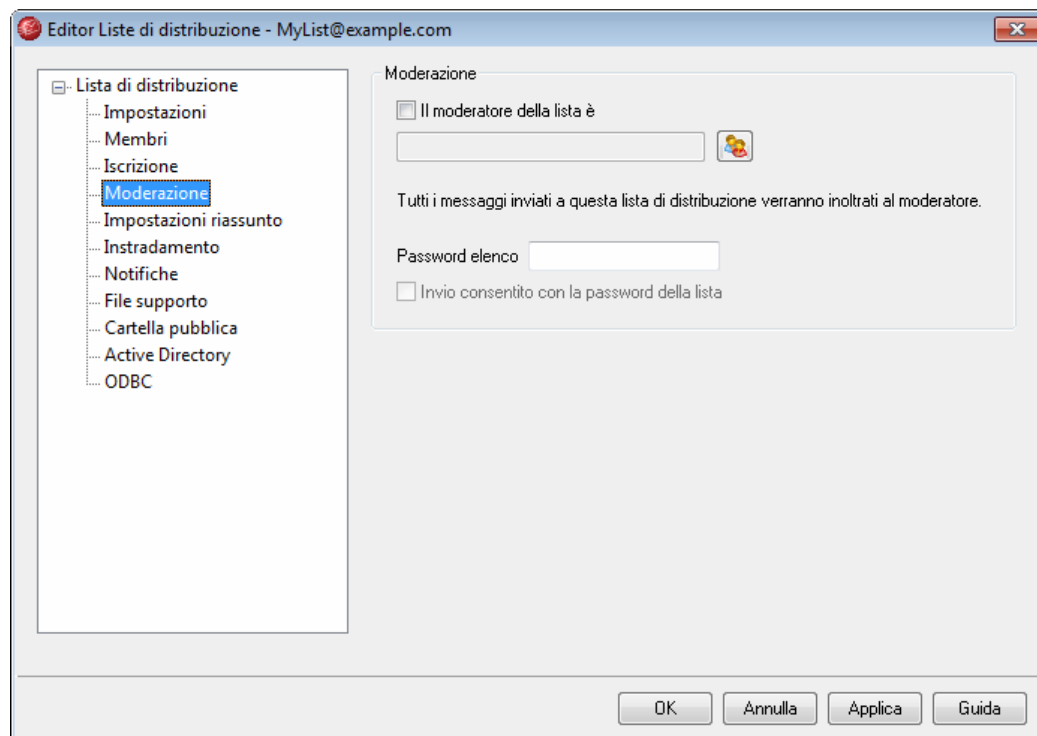
```
List-Unsubscribe: <mailto:<Lista>-Unsubscribe@domain.com>
```

Alcuni client e-mail sono in grado di convertire automaticamente questa intestazione in un pulsante ANNULLA ISCRIZIONE disponibile agli utenti.

Iscrizione/ritiro mediante funzioni di risposta automatica

Per l'iscrizione o il ritiro automatico di membri dalla lista, è possibile utilizzare anche le funzioni di risposta automatica357. A questo scopo, è necessario creare uno o più account di MDaemon il cui unico obiettivo sia quello di aggiungere o rimuovere automaticamente gli indirizzi che hanno inviato un messaggio a tali account, mediante le funzioni di risposta automatica espressamente configurate. Se, ad esempio, esiste una lista di distribuzione denominata "`franco-lista@esempio.com`," è possibile creare un account di MDaemon con il seguente indirizzo: "`join-franco-lista@esempio.com`." Quindi è necessario configurare una risposta automatica per l'account che aggiunga a "`franco-lista@esempio.com`" eventuali indirizzi dai quali abbia ricevuto un messaggio. Così, per unirsi alla lista, è sufficiente inviare un e-mail a "`join-franco-lista@esempio.com`". Questa rappresenta una soluzione semplice, in quanto non è necessario che gli utenti ricordino i particolari comandi e-mail necessari con il metodo *Iscrizione/ritiro mediante comandi e-mail*.

Vedere:

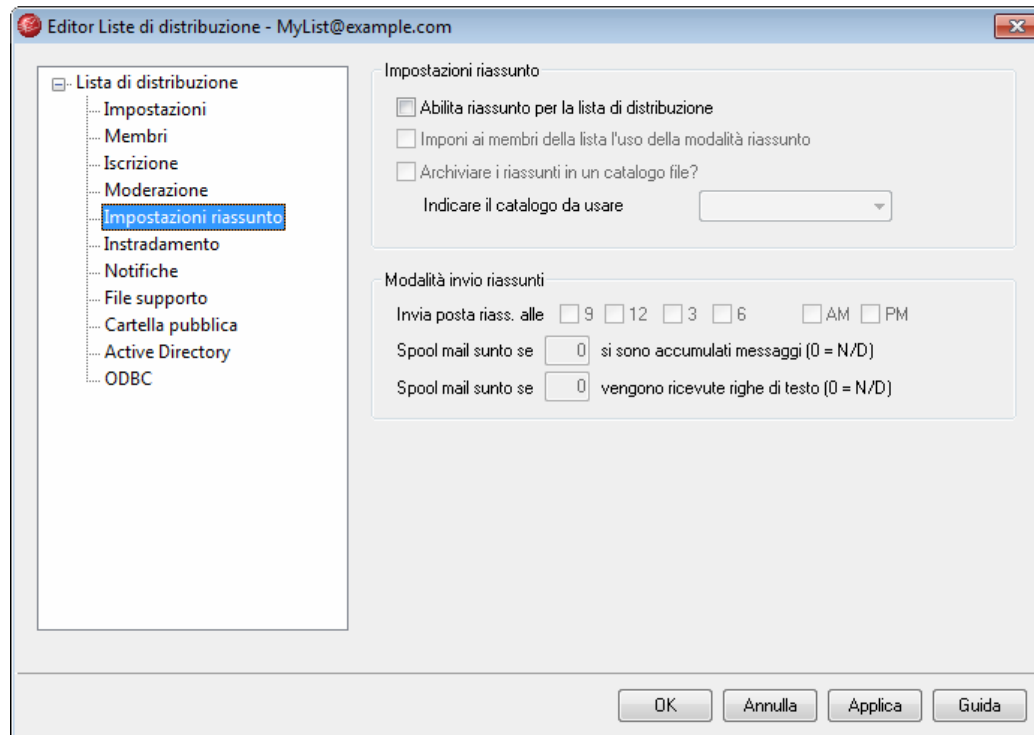
[Iscrizione](434)
[Controllo remoto del server via e-mail](506)
[Risposte automatiche](357)
[Preferenze » Sistema](194)
[Preferenze » Varie](202)

7.1.1.4 Moderazione

Moderazione

Il moderatore della lista è
Se si desidera che la lista venga moderata da un determinato utente, abilitare questa casella e indicare un account. Tutti messaggi delle liste con moderatore vengono inviati al moderatore stesso. Solo il moderatore può sottoporre o inoltrare i messaggi alla lista.

Password elenco
Fare clic per assegnare una password alla lista di distribuzione. Le password delle liste possono essere utilizzate con l'opzione *Invio consentito con la password della lista* oppure per sovrascrivere l'opzione *Limite membri* della schermata Iscrizione[434]. Consentono, inoltre, di accedere alle numerose funzioni descritte nella sezione *Controllo remoto del server via e-mail*[506].

Invio consentito con la password della lista
Se alla lista viene assegnata una password e si abilita questa opzione, per scrivere alla lista è necessario inserire la password all'inizio dell'oggetto del messaggio, anche se alla lista è associato un moderatore qualora questo sia diverso dal mittente.

7.1.1.5 Impostazioni riassunto

Riassunti

Abilita riassunto per la lista distribuzione
Per consentire il supporto dell'attivazione/disattivazione riassunti per la lista di distribuzione, abilitare questa casella. Quando viene attivato il supporto riassunti, una copia di ogni messaggio inviato alla lista di distribuzione viene archiviata in modo che agli iscritti il cui tipo di appartenenza 431 sia impostato su *Riassunto* vengano periodicamente inviati gruppi di messaggi archiviati in formato indicizzato compatto e non i singoli messaggi.

Imponi a tutti i membri della lista di usare la modalità riassunto
Per impostazione predefinita, i membri della lista possono scegliere se ricevere il traffico della lista in formato riassunto o normale. Se si abilita questa casella, verrà utilizzata la modalità riassunto, a prescindere dalla selezione dell'utente.

Archiviare i riassunti in un catalogo file / Indicare il catalogo da usare
Queste opzioni consentono di includere i messaggi di riassunto in un catalogo file, così da poterne raccogliere numeri arretrati in futuro. MDaemon genera un archivio

univoco per ciascun riassunto e lo include nel catalogo specificato.

Per informazioni più dettagliate sull'uso dei cataloghi, vedere: Editor cataloghi 480.

Modalità invio riassunti

Le seguenti opzioni determinano la frequenza e le circostanze in cui gli iscritti alla lista, le cui impostazioni lo prevedono, riceveranno la posta in formato riassunto. Le opzioni operano tutte in modo indipendente le une dalle altre, così che l'invio di un riassunto può essere determinato da alcune o da tutte le impostazioni.

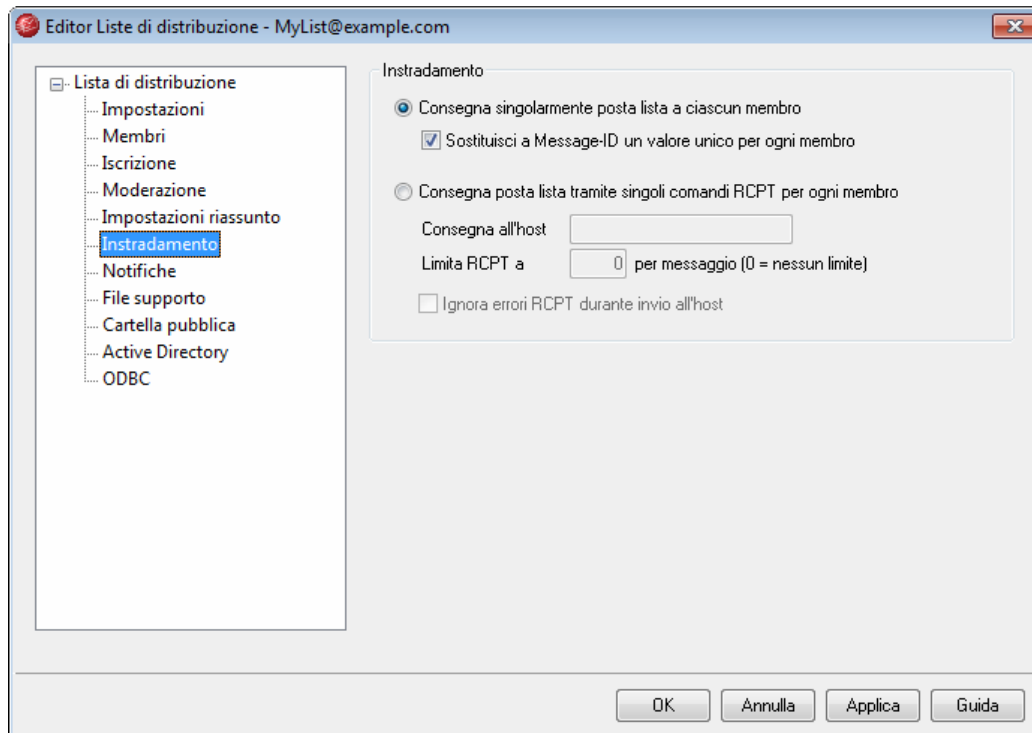
Invia posta riass. alle 9, 12, 3, 6 AM e/o PM
Questa opzione consente di pianificare la frequenza di invio dei riassunti. Abilitando tutte le caselle di questa opzione, i riassunti verranno inviati ogni tre ore oltre che in base agli eventi attivati dalle opzioni successive.

Spool mail sunto se si sono accumulati [XX] messaggi (0 = N/D)
Se si desidera che i riassunti vengano inviati automaticamente quando si supera la soglia di un determinato numero di messaggi, specificarne il numero. Inserire "0" se non si desidera usufruire di questa opzione. "0" è l'impostazione predefinita.

Spool mail sunto se vengono ricevute [XX] righe di testo (0 = N/D)
Se si inserisce un valore, i riassunti vengono inviati appena superato il numero di righe di testo specificato. Inserire "0" se non si desidera usufruire di questa opzione. "0" è l'impostazione predefinita.

Vedere:

Membri 431
Editor cataloghi 480
Controllo remoto del server via e-mail 506

7.1.1.6 Instradamento

Instradamento

Consegna singolarmente posta lista a ciascun membro
Se si seleziona questa opzione, viene creata una copia distinta dei messaggi ricevuti per la distribuzione alla lista che viene, poi, recapitata ai singoli membri. Ciò determina la creazione di numerosi messaggi che si riflette sulle prestazioni del server, in base alla dimensione della lista e al carico del server.

Sostituisci a Message-ID un valore unico per ogni membro
Se si imposta MDaemon per la creazione di una copia distinta di ogni messaggio per i singoli membri, con questa casella di controllo è possibile assegnare a tutti i messaggi un ID univoco.

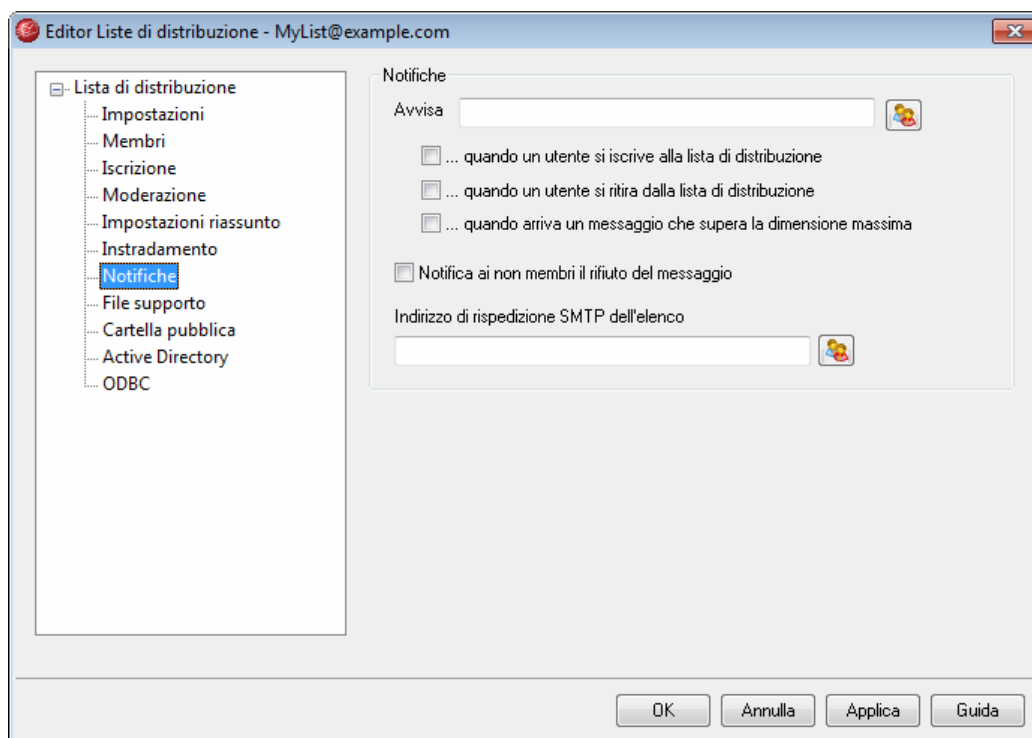
Consegna posta lista tramite singoli comandi RCPT per ogni membro
Se questa casella di controllo è selezionata, anziché inviare messaggi ai singoli membri, MDaemon instrada una sola copia di ciascun messaggio della lista all'host intelligente specificato. Durante la sessione SMTP con l'host specificato, questo metodo utilizza più istruzioni `RCPT TO`.

Consegna all'host
Consente di indicare l'host intelligente al quale trasmettere tutti i messaggi della lista da consegnare, utilizzando istruzioni RCPT TO per ogni membro.

Limita RCPT a XX per messaggio (0=nessun limite)
Alcuni host stabiliscono un limite sul numero di istruzioni `RCPT TO` che si possono utilizzare per l'instradamento di una singola copia del messaggio. Se si specifica

tale limite in questo campo, MDaemon crea delle copie supplementari del messaggio e suddivide la lista in gruppi più ridotti. Quindi, consegna il messaggio a tali gruppi, evitando così di superare il limite specificato. Questa opzione è simile alla precedente *Consegna singolarmente posta lista a ciascun membro*, ma crea un numero di copie inferiore e invia ogni copia a un gruppo di indirizzi, anziché generare copie distinte per ogni membro.

Ignora errori RCPT durante invio all'host
Poiché per determinati domini alcuni host intelligenti rifiutano di collocare la posta nella coda o di eseguirne lo spool, la consegna alla lista mediante instradamento potrebbe generare numerosi inconvenienti. A causa di un codice di errore restituito dall'host intelligente come risultato del rifiuto, di solito MDaemon abbandona il tentativo di consegna. Selezionando questa opzione, MDaemon ignora i codici di errore restituiti dall'host intelligente durante la consegna della posta della lista instradata consentendo, così, ai membri accettati di ricevere il messaggio della lista.

7.1.1.7 Notifiche

Notifiche

Notifica
Questa opzione consente di specificare un indirizzo a cui inviare una notifica quando si verificano gli eventi selezionati.

... quando un utente si iscrive alla lista di distribuzione
Abilitare questa casella per inviare una nota all'indirizzo indicato per ogni iscrizione alla lista di distribuzione.

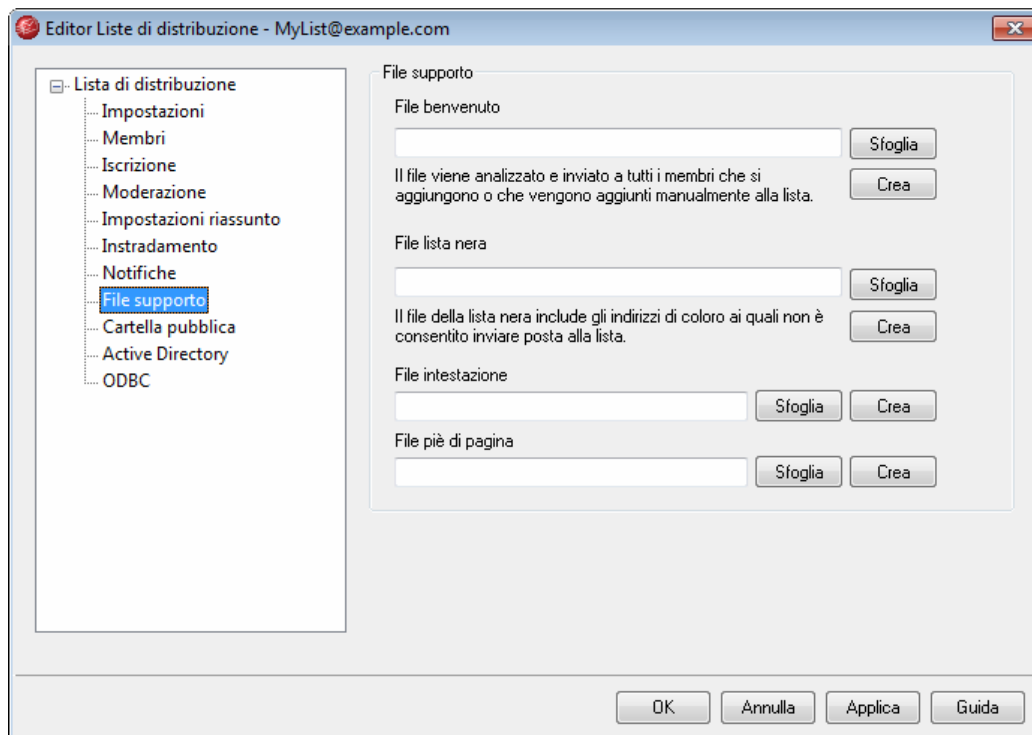
... quando un utente si ritira dalla lista di distribuzione
Abilitare questa casella per inviare una nota all'indirizzo indicato per ogni ritiro dalla lista di distribuzione.

... quando arriva un messaggio che supera la dimensione massima
Abilitando questa casella è possibile inviare una nota all'indirizzo indicato ogni volta che alla lista di distribuzione viene inviato un messaggio superiore al limite *Rifiuta messaggi lista superiori a XX KB* indicato in Impostazioni429.

Notifica ai non membri il rifiuto del messaggio
Se questa opzione è abilitata, quando gli utenti inviano messaggi a una lista privata di cui non fanno parte, ricevono un apposito avviso da MDaemon, nonché istruzioni per un'eventuale iscrizione alla lista. Per definire una lista privata, utilizzare l'opzione *Invio posta alla lista consentito solo ai membri* di Impostazioni429.

Posta restituita

Indirizzo di rispedizione SMTP dell'elenco
Questa opzione consente di specificare l'indirizzo di rispedizione della posta o dei messaggi sullo stato di consegna generati dal traffico della lista. Ad esempio, una lista di distribuzione con 100 destinatari può includere dieci indirizzi a cui non è possibile recapitare i messaggi perché l'indirizzo è cambiato, il server è fuori servizio o per altri motivi. Il sistema SMTP genera un messaggio per notificare tale impossibilità di consegna e lo invia al mittente del messaggio. Questa opzione consente di indicare l'indirizzo che riceverà questi messaggi relativi alle liste di distribuzione. È anche possibile indicare che nessuno li riceva. In questo caso MDaemon inserirà i messaggi della lista nel flusso di posta, in modo che non sia possibile inviare un messaggio di risposta. L'indirizzo NON può coincidere con l'indirizzo della lista di distribuzione.

7.1.1.8 File di supporto

File di supporto

File benvenuto
Se indicato, il file presente in questo campo viene elaborato e il suo contenuto inviato a tutti i nuovi membri subito dopo l'iscrizione. Nel file di benvenuto per un nuovo iscritto è possibile utilizzare le seguenti macro:

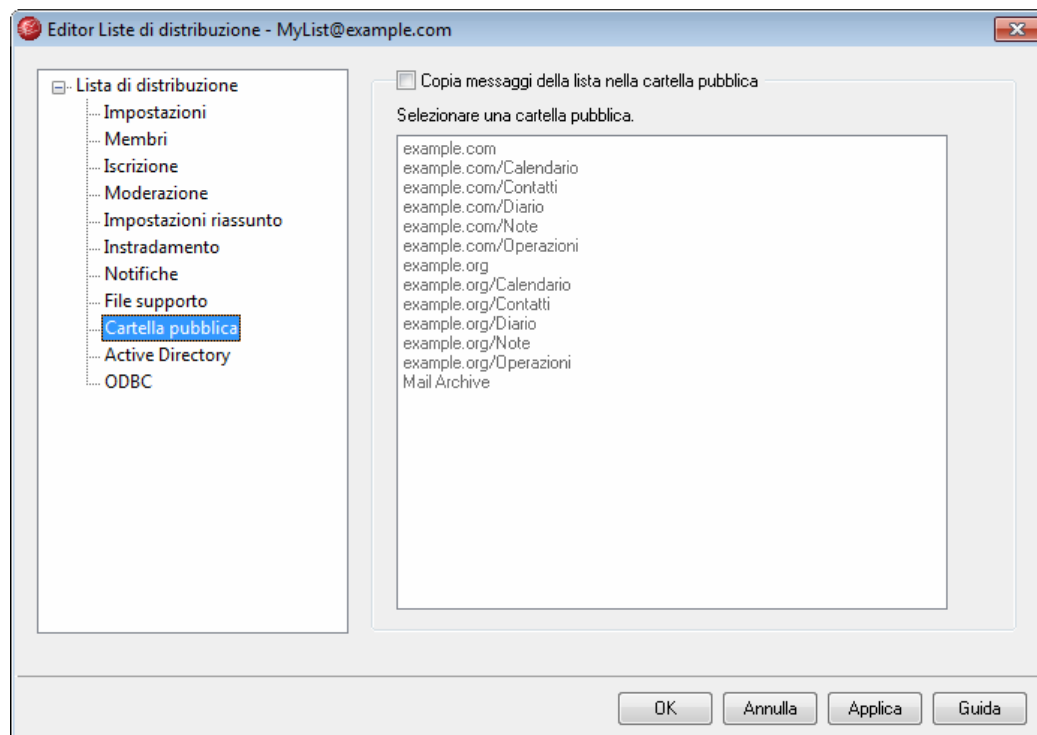
`$PRIMARYDOMAIN$`	Questa macro restituisce il nome di dominio predefinito di MDaemon, indicato nella schermata Dominio 41.
`$PRIMARYIP$`	Questa macro restituisce l'indirizzo IP associato al dominio predefinito di MDaemon.
`$MACHINENAME$`	Questa macro restituisce il contenuto dell'opzione FQDN indicata nello schermo Dominio.
`$LISTEMAIL$`	Questa macro consente di visualizzare l'indirizzo di posta elettronica della lista. Esempio: `NomeLista@esempio.com`
`$LISTNAME$`	Questa macro consente di visualizzare il nome della lista di distribuzione. Esempio: `NomeLista`
`$LISTDOMAIN$`	Questa macro restituisce il dominio della lista di distribuzione. Esempio: `esempio.com`

`%SETSUBJECT%` Questa macro consente di indicare un oggetto alternativo per il messaggio di benvenuto. Il testo dell'oggetto specificato può includere altre macro di lista come `$LISTEMAIL$`. Esempio: `%SetSubject%=Benvenuto in $LISTNAME$.`

File lista nera
Se indicato, il file presente in questo campo viene utilizzato per sopprimere i messaggi inviati da determinati utenti.

File intestazione/piè di pagina
Il contenuto dei file specificati in questi campi viene utilizzato sotto forma di intestazione e/o piè di pagina per i messaggi della lista.

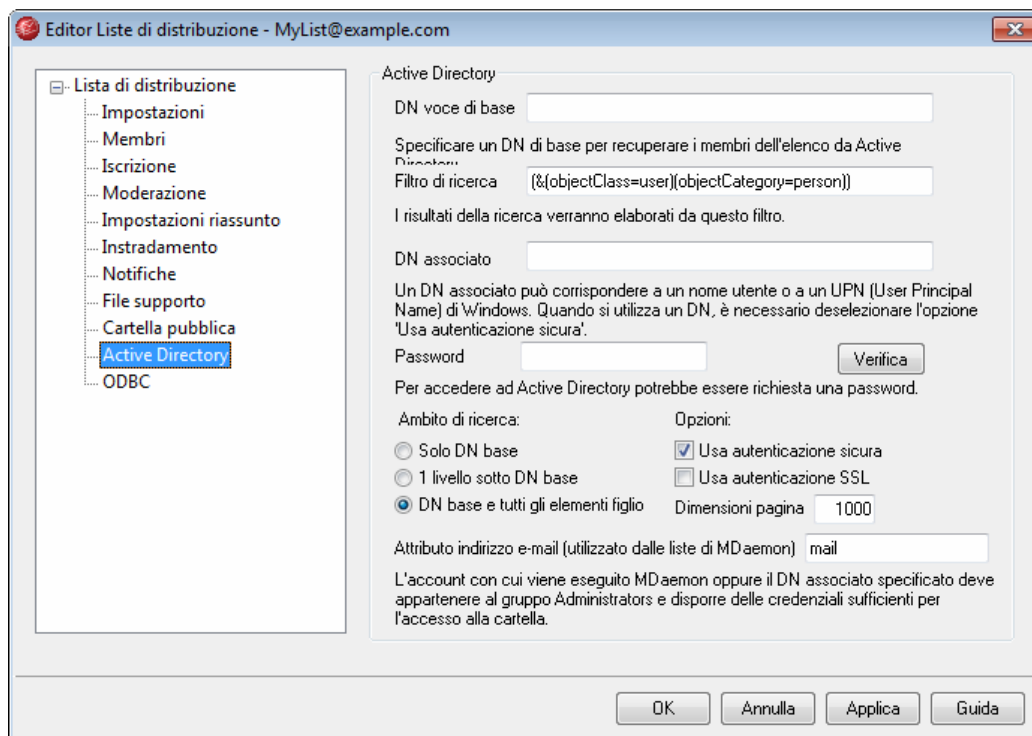
Crea
Per creare un nuovo file, fare clic sul pulsante *Crea* corrispondente al file da creare, specificare un nome e, quindi, fare clic su *Apri*. In tal modo, il file di nuova creazione viene aperto in Blocco note e può essere modificato.

7.1.1.9 Cartella pubblica

MDaemon consente di utilizzare le Cartelle IMAP pubbliche 75 con le liste di distribuzione. Le cartelle pubbliche sono cartelle aggiuntive che, diversamente dalle cartelle IMAP personali di solito accessibili a un solo utente, possono essere utilizzate da più utenti IMAP (Internet Message Access Protocol). Utilizzando le opzioni di questa schermata, tutti i messaggi indirizzati alla lista di distribuzione vengono

automaticamente copiati in una delle cartelle pubbliche.

Copia messaggi della lista nella cartella pubblica
Abilitare questo comando se si desidera che i messaggi della lista vengano copiati in una delle cartelle pubbliche, oltre a essere consegnati alla lista.

Seleziona cartella pubblica
Selezionare la cartella pubblica che si desidera associare ai messaggi della lista.

7.1.1.10 Active Directory

Utilizzare le opzioni di questa schermata se si desidera recuperare gli indirizzi dei membri dell'elenco da Active Directory.

Active Directory

DN voce di base
Specificare il DN (Distinguished Name), ossia il punto iniziale nella struttura DIT (Directory Information Tree) a partire dal quale MDaemon esegue la ricerca degli indirizzi di Active Directory. Utilizzando "`LDAP://rootDSE`" in questa opzione la ricerca viene eseguita a partire dalla directory principale DSE, che rappresenta la voce di livello più alto nella gerarchia di Active Directory. L'indicazione di un punto iniziale più accurato e prossimo alla posizione degli account utente o del gruppo desiderato di indirizzi nella struttura di Active Directory può ridurre il tempo richiesto dalla ricerca nella struttura DIT. Lasciare vuoto questo campo se non si desidera recuperare alcun indirizzo della lista dalla Active Directory.

Filtro di ricerca
Rappresenta il filtro di ricerca LDAP utilizzato per le ricerche in Active Directory. Utilizzare questo filtro per consentire a MDaemon di localizzare con maggiore accuratezza gli account utente desiderati o gli indirizzi che si desidera considerare come iscritti alla lista.

DN associato
Rappresenta il DN utilizzato da MDaemon per l'associazione ad Active Directory mediante LDAP. Per l'associazione, Active Directory consente l'uso di un account Windows o di un UPN.

Quando si utilizza un DN invece di un ID utente Windows per questa opzione, è necessario disattivare/deselezionare l'opzione "*Utilizza autenticazione sicura*".

Password
È la password corrispondente al DN o all'ID utente Windows indicato nell'opzione *DN associato*.

Verifica
Fare clic su questo pulsante per eseguire una verifica della configurazione di Active Directory.

Ambito di ricerca:

Rappresenta l'ambito, ossia la portata delle ricerche Active Directory.

Solo DN base
Scegliere questa opzione se si desidera limitare la ricerca al solo DN base indicato in precedenza. In questo modo, la ricerca nella struttura DIT non verrà eseguita oltre tale punto.

1 livello inferiore al DN base
Utilizzare questa opzione se si desidera estendere la ricerca nella struttura DIT di Active Directory ad un livello inferiore al DN specificato.

DN base e tutti gli elementi figlio
Con questa opzione, l'ambito della ricerca viene esteso dal DN fornito a tutti i relativi figli, fino all'ultimo elemento figlio del DIT.

Opzioni:

Usa autenticazione sicura
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione sicura durante l'esecuzione di ricerche in Active Directory. Non è possibile utilizzare questa opzione se nell'opzione *DN associato* indicata in precedenza viene specificato un DN anziché un ID utente Windows.

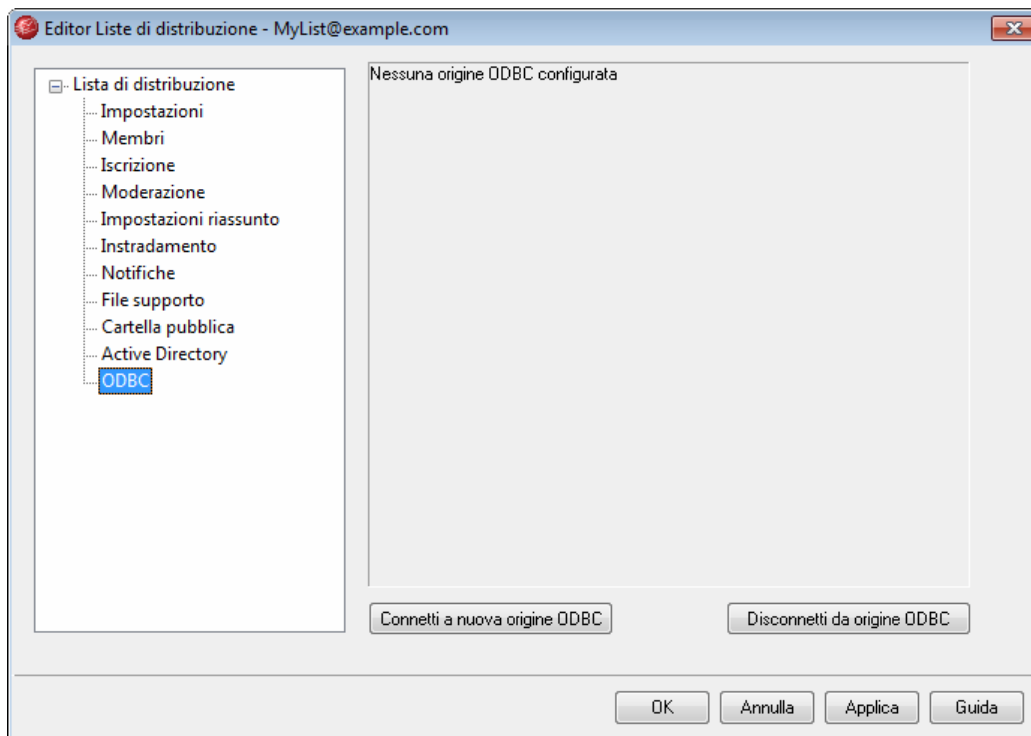
Usa autenticazione SSL
Fare clic su questa casella di controllo se si desidera utilizzare l'autenticazione SSL durante l'esecuzione di ricerche in Active Directory.

Dimensioni pagina
Se l'interrogazione di Active Directory restituisce un numero elevato di voci, queste vengono raggruppate in "pagine" diverse per consentire il recupero di tutti i risultati. Questa impostazione rappresenta il numero massimo di voci da includere per ogni pagina.

L'utilizzo di questa opzione richiede la presenza di un server e di un'infrastruttura SSL nella rete Windows e in Active Directory. Se non si è certi dell'impostazione della rete o per ulteriori informazioni sulla possibilità di attivare questa opzione, rivolgersi al proprio reparto IT.

Attributo indirizzo e-mail

È necessario utilizzare questo campo per specificare l'attributo in cui sarà inserito l'indirizzo e-mail utilizzato dalla lista. Ad esempio, se si specifica "`Mail`" in questo campo, ogni account Active Directory da considerare membro della lista deve avere l'attributo "`Mail`" e l'attributo deve contenere un indirizzo e-mail.

7.1.1.11 ODBC

Questa funzionalità consente di gestire l'elenco degli appartenenti alle liste di distribuzione mediante un database compatibile con ODBC. La schermata ODBC dell'editor delle liste di distribuzione consente di selezionare la corrispondenza con origini dati, tabelle e campi per il collegamento alla lista. Quando arriva un messaggio per la propria lista, vengono eseguite automaticamente una o più interrogazioni SQL e gli indirizzi e-mail risultanti vengono considerati come appartenenti alla lista.

È inoltre possibile aggiungere, rimuovere e modificare i membri della lista presenti nel database con qualsiasi applicazione di database compatibile con ODBC.

ODBC

In questa sezione vengono visualizzate le proprietà ODBC impostate per la lista di distribuzione. Vengono inoltre riportate le corrispondenze tra i campi del database e le interrogazioni SQL configurate per indicare lo stato di appartenenza di ogni membro: modalità Normale, Solo invio, Solo lettura e/o Riassunto.

Connetti a nuova origine ODBC
Questo pulsante consente di avviare Selezione guidata ODBC per la scelta dell'origine dati di sistema da utilizzare per la lista di distribuzione.

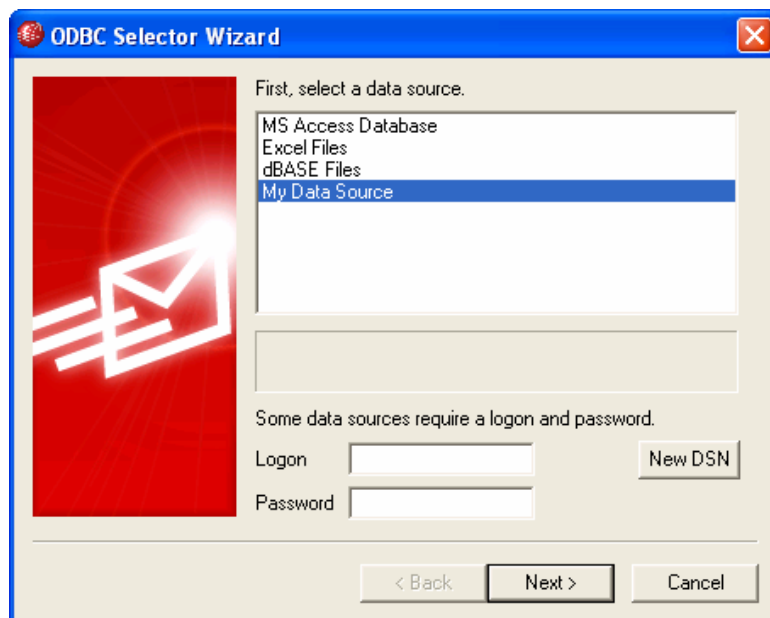
Disconnetti da origine ODBC
Fare clic su questo pulsante per scollegare la lista dall'origine dati ODBC elencata.

Vedere:

Configurazione di un'origine dati di sistema ODBC per una lista di distribuzione 449
Creazione di una nuova origine dati di sistema 452

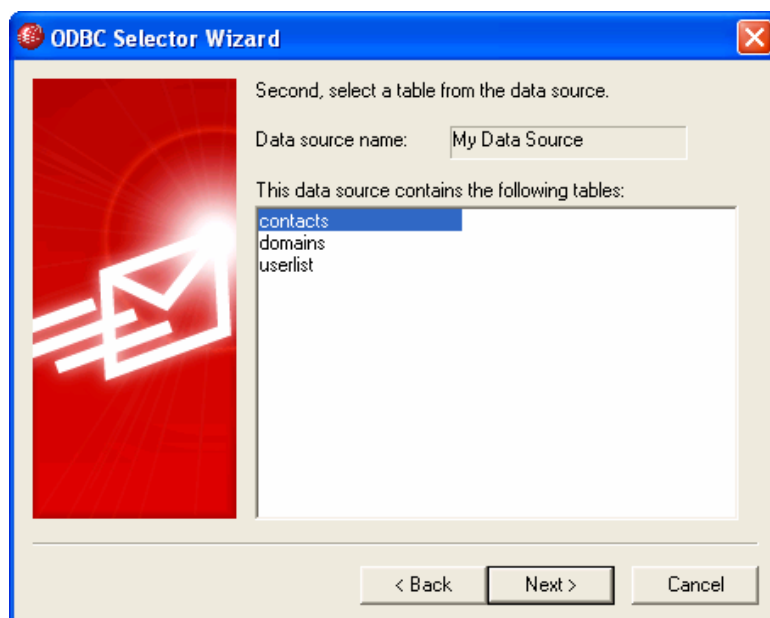
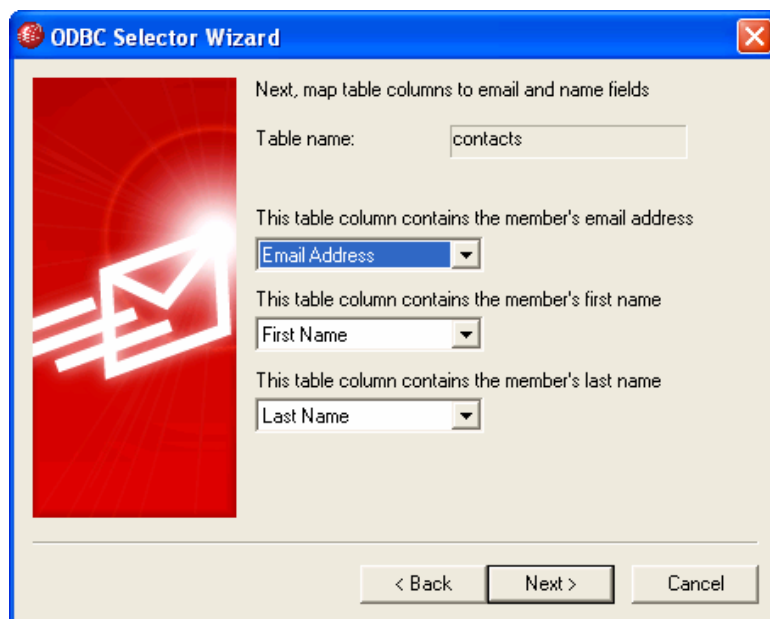
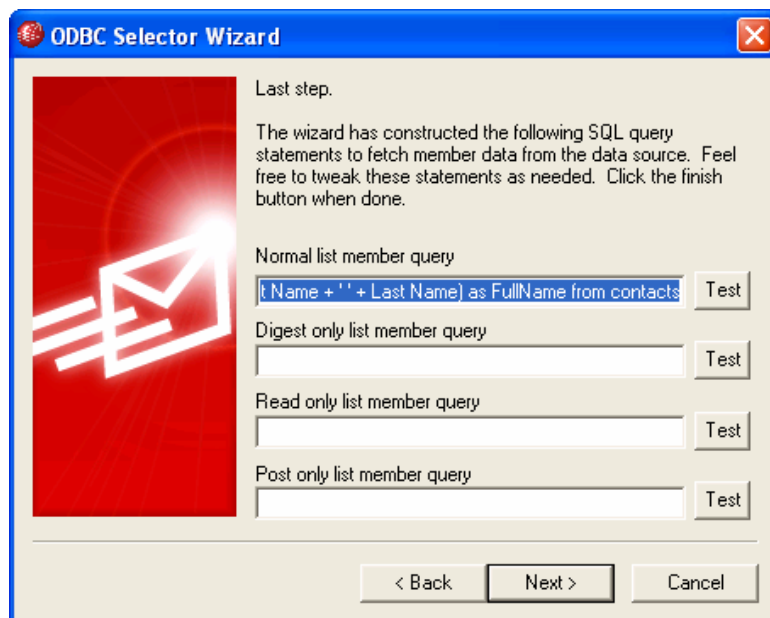
7.1.1.11.1 Configurazione di un'origine dati ODBC

Per utilizzare un database ODBC con una lista di distribuzione, procedere come segue.

1. Nella schermata ODBC 448 dell'editor delle liste di distribuzione, fare clic su Connetti a nuova origine ODBC per aprire Selezione guidata ODBC.

2. Selezionare l'origine dati desiderata per la lista di distribuzione. Se questa non è presente nell'elenco, fare clic su Nuovo DSN e seguire le indicazioni fornite in **Creazione di una nuova origine dati ODBC** 452.

3. Se necessario, inserire l'ID accesso e la Password dell'origine dati.

4. Scegliere Avanti.

5. Nell'origine dati deve essere presente almeno una tabella contenente i campi relativi all'indirizzo di posta elettronica e al nome. Se sono disponibili più tabelle di qualificazione, selezionare quella desiderata e scegliere Avanti. Altrimenti, scegliere Annulla per uscire dalla Selezione guidata ODBC e, prima di proseguire, aggiungere una tabella al database in questione utilizzando l'applicazione di database.

6. Nelle caselle di riepilogo a discesa indicare i campi della tabella che corrispondono all'**indirizzo di posta elettronica**, al **nome** e al **cognome**. Scegliere Avanti.

7. Selezione guidata ODBC crea un'istruzione di interrogazione SQL in base a quanto selezionato nel **passaggio 6.** I risultati verranno utilizzati per recuperare i dati dei membri della lista normale dal database. È possibile modificare questa istruzione nel modo desiderato, nonché includere altre istruzioni di interrogazione nei controlli rimanenti per consentire ai membri di ricevere i messaggi in modalità Riassunto e per indicare quale membri siano in modalità Solo lettura o Solo invio. Accanto a ogni controllo è presente un pulsante Test che consente di esaminare le istruzioni di interrogazione per verificare che recuperino i dati desiderati. Al termine della configurazione delle istruzioni di interrogazione, fare clic su Avanti.

8. Scegliere Fine.

Vedere:

Editor Liste di distribuzione » ODBC 448

Creazione di una nuova origine dati ODBC 452

7.1.1.11.2 Creazione di una nuova origine dati ODBC

Per creare una nuova origine dati di sistema ODBC da utilizzare per la lista di distribuzione, procedere come segue.

1. Nella schermata ODBC 448 dell'editor delle liste di distribuzione, fare clic su Connetti a nuova origine ODBC per aprire Selezione guidata ODBC.

2. Fare clic su Nuovo DSN per aprire la finestra di selezione dell'origine dati.

3. Passare alla scheda Origine dati computer e fare clic su Nuova per aprire la finestra di dialogo Crea nuova origine dati.

4. Selezionare Origine dati di sistema e fare clic su Avanti.

5. Selezionare il driver di database desiderato per l'origine dati, quindi fare clic su Avanti.

6. Fare clic su Fine per visualizzare la finestra di dialogo per l'impostazione dello specifico driver. L'aspetto di questa finestra di dialogo varia a seconda del driver selezionato. Quella visualizzata di seguito è la finestra di dialogo relativa alle impostazioni di accesso Microsoft.

7. Indicare un valore per la nuova origine nel campo Nome origine dati e fornire le altre informazioni richieste dalla finestra di dialogo relativa allo specifico driver, quali la creazione o l'indicazione di un database, la scelta di una directory o di un server e così via.

8. Fare clic su OK per chiudere la finestra di dialogo del driver.

9. Fare clic su OK per chiudere la finestra di selezione dell'origine dati.

Per ulteriori informazioni, vedere:

ODBC - Liste di distribuzione 448
Configurazione di un'origine dati di sistema ODBC per una lista di distribuzione 449

Sezione VIII

8 Menu Gateway

8.1 Gateway di dominio

Gateway Editor 459 è una funzione di MDaemon PRO alla quale si accede dalla selezione di menu Gateway » Nuovo gateway o Gateway » Modifica gateway. Questa funzionalità offre un secondo livello di supporto, limitato ma utile, per l'hosting di più domini o come server di posta di backup.

Di seguito viene descritto un esempio di utilizzo di questa funzionalità.

> Si supponga di assumere la funzione di server di backup o di mail-drop per conto terzi, ricevendone le e-mail in entrata e memorizzandole in una cartella del server, senza peraltro eseguire l'hosting completo del dominio gestendone i singoli account utente. Il nome di questo dominio di esempio sarà "`azienda.com`".
>
> La prima operazione consiste nell'inserire "`azienda.com`" nell'opzione *Nome dominio* della schermata Dominio. Quindi, si seleziona la cartella nella quale memorizzare la posta del dominio in entrata. Tutta la posta che MDaemon riceve per il dominio verrà separata dal flusso della posta principale e collocata in questa cartella, indipendentemente dai destinatari specifici dei messaggi.
>
> Successivamente, è necessario indicare i metodi di raccolta o di consegna desiderati affinché le i messaggi e-mail del dominio pervengano al server di posta effettivo in cui si trovano i relativi account utente. Sono disponibili tre metodi per eseguire questa operazione: utilizzare l'opzione *Consegna i messaggi memorizzati ogni volta che MDaemon elabora la posta remota* della schermata Dominio 460, utilizzare le opzioni di annullamento dell'accodamento 467 o impostare un account per il dominio nella schermata Account 470.
>
> Infine, è probabile che sia necessario modificare le impostazioni DNS di `azienda.com` in modo da indicare il server MDaemon come host MX del dominio.

Esistono molte altre funzioni e opzioni per i gateway, ma quello dell'esempio precedente rappresenta un tipico gateway di base. Tuttavia, se si desidera una configurazione atipica può essere necessario eseguire operazioni diverse, ad esempio se si desidera utilizzare un nome di dominio inesistente in Internet come "`azienda.mail`." La ricezione di messaggi con un nome di dominio altrimenti non valido come questo è possibile, ma è necessario che tale nome sia "nascosto" in un indirizzo di Dominio predefinito 41. Questo metodo consente di creare indirizzi che possano attraversare il dominio predefinito e arrivino al gateway. Se, ad esempio, il dominio predefinito è `esempio.com` e si dispone di un gateway per `azienda.mail`, è possibile inviare un messaggio a "`bob@azienda.mail`" utilizzando l'indirizzo "`bob{azienda.mail}@esempio.com`." Poiché "`esempio.com`" è il dominio registrato ospitato da MDaemon, tale messaggio verrà recapitato correttamente ma, dopo aver ricevuto il messaggio in questo formato, MDaemon convertirà l'indirizzo in "`bob@azienda.mail`" e lo recapiterà alla cartella specificata per il gateway. Il metodo più semplice consiste, naturalmente, nel registrare un nome di dominio valido per il gateway e quindi indirizzarne il record DNS o MX a `esempio.com`.

Vedere:

[Gateway Editor](459)
[Dominio predefinito](41)
[Domini aggiuntivi](114)

8.1.1 Gateway Editor

Per accedere a Gateway Editor è possibile fare clic su Gateway » Nuovo gateway o su Gateway » Modifica gateway nella barra dei menu di MDaemon. Sono disponibili le schermate seguenti:

Dominio 460
Questa finestra di dialogo consente di definire il nome del dominio per il quale MDaemon funge da gateway o da server di backup e di indicare la cartella utilizzata per memorizzare i messaggi del dominio.

Verifica 462
Se il server del dominio remoto esegue l'aggiornamento di un server LDAP o Active Directory con tutte le caselle postali, tutte le liste di distribuzione e tutti gli alias in esso contenuti o se include un server Minger per la verifica degli indirizzi remoti, è possibile utilizzare questa finestra di dialogo per specificare il server in questione e verificare la validità degli indirizzi dei destinatari dei messaggi in arrivo. Se un indirizzo non è valido, il messaggio viene respinto. Grazie a questo metodo, non è necessario attenersi all'assunto che tutti i destinatari dei messaggi di un dominio siano validi.

Inoltro 466
Questa finestra di dialogo consente di specificare l'host o indirizzo a cui deve essere inoltrata la posta del dominio in arrivo. Sono inoltre disponibili opzioni che consentono di specificare la porta per l'inoltro dei messaggi e di salvare a livello locale una copia dei messaggi.

Annullamento dell'accodamento 467
Le opzioni di questa finestra di dialogo consentono di specificare se MDaemon deve rispondere alle richieste ETRN e ATRN effettuate per conto del dominio al fine di annullare l'accodamento dei messaggi. È inoltre possibile configurare diverse altre opzioni relative all'annullamento dell'accodamento.

Account 470
Tramite questa scheda, è possibile creare l'account utente POP3 o IMAP che potrà accedere alla posta memorizzata del dominio. Utilizzando il nome e la password assegnati in questa scheda, un "agente utente" (Mail User Agent, MUA) come ad esempio un normale client di posta o un altro server MDaemon può accedere alla casella postale del dominio e raccoglierne il contenuto.

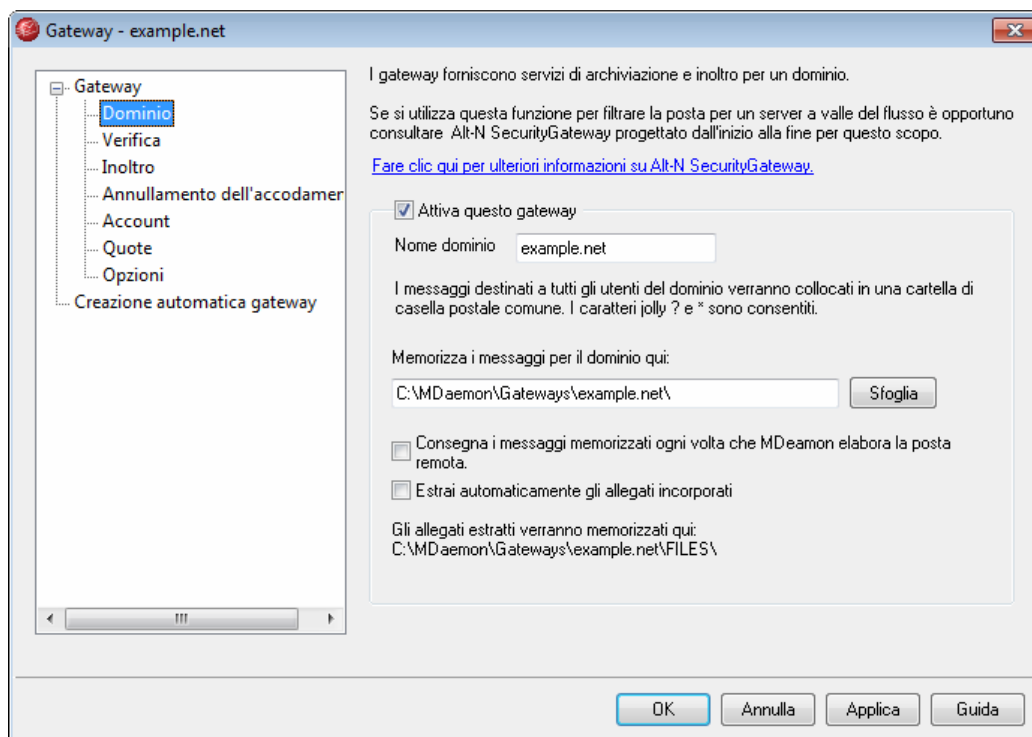
Quote 471
Questa finestra di dialogo consente di impostare i limiti relativi alla quantità di spazio

su disco utilizzabile dal dominio e al numero massimo di messaggi memorizzabili.

Opzioni 472
Questa schermata contiene numerose altre opzioni che verranno applicate al gateway di dominio selezionato. È possibile, ad esempio, abilitare o disabilitare la scansione AntiVirus e AntiSpam per il gateway, specificare se per l'annullamento dell'accodamento della posta è richiesta l'autenticazione, definire la password per l'autenticazione, specificare restrizioni per le connessioni provenienti da indirizzi IP definiti e così via.

Per ulteriori informazioni, vedere:

Gateway di dominio 458

8.1.1.1 Dominio

Dominio gateway

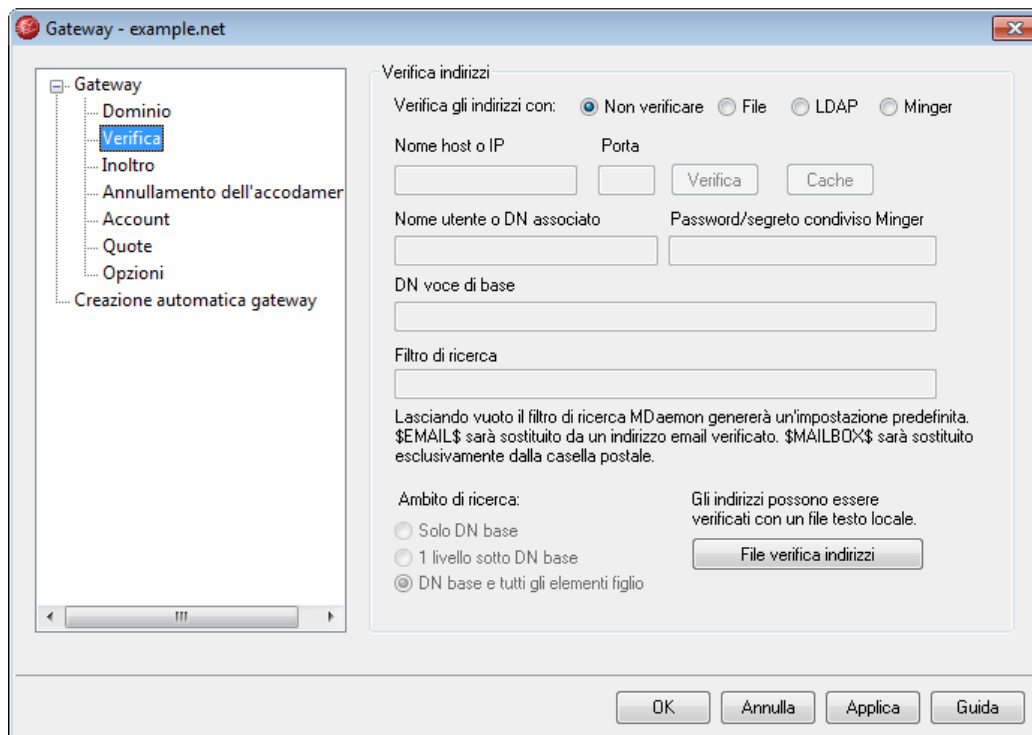
Attiva questo gateway
Per attivare il dominio gateway, selezionare questa casella.

Nome dominio
Inserire il nome del dominio per cui si desidera che MDaemon svolga funzioni di gateway e-mail o di ricezione posta.

Memorizza i messaggi per il dominio qui
Inserire la directory nella quale memorizzare la posta in entrata del dominio. Tutti i messaggi verranno memorizzati nella stessa cartella, indipendentemente dai singoli destinatari cui i messaggi sono indirizzati.

Consegna i messaggi memorizzati ogni volta che MDaemon elabora la posta remota
Solitamente, quando MDaemon riceve la posta diretta a uno dei relativi gateway, la memorizza fino a quando il dominio si connette a MDaemon per raccoglierla. In alcune situazioni può essere opportuno che MDaemon tenti di consegnare la posta direttamente via SMTP, senza attendere che venga raccolta dal dominio. Quando questa opzione è abilitata, MDaemon tenta di consegnare i messaggi del dominio ogni volta che viene elaborata la posta remota. La casella postale del gateway opererà temporaneamente come coda remota e verrà eseguito un tentativo di consegna. Tutti i messaggi che non possono essere consegnati rimarranno nella casella postale del gateway finché non vengono raccolti dal dominio oppure verranno consegnati in un secondo momento, ma non saranno spostati né nella coda remota, né nel sistema tentativi. Se, tuttavia, il DNS del dominio non è configurato correttamente oppure se la configurazione di MDaemon prevede che trasmetta tutti i messaggi in uscita a un altro host per la consegna, tali messaggi potrebbero rimanere intrappolati in un loop di posta e, successivamente, essere considerati come posta impossibile da consegnare.

Estrai automaticamente gli allegati incorporati
Alcuni sistemi di posta richiedono che i file allegati vengano estratti prima che i messaggi siano sottoposti al flusso di posta. Per facilitare questa operazione, MDaemon è in grado di estrarre automaticamente gli allegati MIME in entrata e di collocarli nella sottocartella `\Files\` della cartella dei messaggi del dominio. Se si desidera l'estrazione automatica degli allegati, abilitare questa casella.

8.1.1.2 Verifica

Un problema diffuso con i gateway di dominio e i servizi di ricezione della posta consiste nel non disporre generalmente di un sistema in grado di stabilire la validità del destinatario del messaggio in entrata. Se, ad esempio, si opera in qualità di gateway per `esempio.com` e arriva un messaggio per `franco@esempio.com`, non è possibile stabilire se, nel server e-mail di esempio.com, esista effettivamente una casella postale, un alias o una lista di distribuzione corrispondente all'indirizzo. Pertanto, l'unica possibilità consiste nel considerare l'indirizzo valido e accettare il messaggio. Poiché, inoltre, gli "spammer" inviano spesso messaggi a numerosi indirizzi non validi, questo problema può far sì che il gateway accetti una elevata quantità di posta indesiderata.

MDaemon include un metodo per prevenire questo problema mediante la verifica dell'indirizzo del destinatario. Se il server del dominio remoto esegue l'aggiornamento di un server LDAP o Active Directory con tutte le caselle postali, tutte le liste di distribuzione e tutti gli alias in esso contenuti o se include un server Minger per la verifica degli indirizzi remoti, è possibile utilizzare le opzioni di questa schermata per specificare il server LDAP, Active Directory o Minger nei quali sono memorizzate tali informazioni. In questo modo, all'arrivo di un messaggio per `esempio.com`, è possibile ricercare l'indirizzo del destinatario nell'altro server al fine di stabilirne la validità.

Verifica indirizzi

Verifica gli indirizzi con:

Non verificare
Scegliere questa opzione se non si desidera utilizzare la verifica degli indirizzi email per il gateway di dominio. MDaemon considererà validi tuti gli indirizzi dei destinatari dei messaggi in arrivo per il dominio, poiché non disporrà di alcun metodo per identificare gli indirizzi effettivamente esistenti per il dominio.

File

Scegliere questa opzione se si desidera utilizzare il file `GatewayUsers.dat` come elenco degli indirizzi al fine di verificare la validità dei destinatari dei messaggi in arrivo per il dominio. Si tratta di un elenco globale di indirizzi che viene applicato a tutti i gateway di dominio. Il file viene utilizzato come ulteriore fonte di indirizzi validi anche se si utilizza uno degli altri metodi di verifica disponibili. Se si utilizza l'opzione *File*, tuttavia, il file rappresenta l'unico metodo di verifica utilizzato. È inoltre possibile aprire e modificare l'elenco degli indirizzi validi selezionando il pulsante *File verifica indirizzi*.

LDAP

Scegliere questa opzione per attivare la verifica degli indirizzi remoti mediante LDAP o Active Directory. All'arrivo di un messaggio per un dominio remoto, il server LDAP o Active Directory viene interrogato per verificare la validità dell'indirizzo del destinatario. Se l'indirizzo non è valido, il messaggio verrà respinto. Qualora MDaemon non sia in grado di connettersi al server LDAP o AD, l'indirizzo verrà considerato comunque valido.

Minger

Scegliere questa opzione se si desidera eseguire una ricerca dell'indirizzo del destinatario del dominio nel server Minger del dominio. Qualora MDaemon non sia in grado di connettersi al server, l'indirizzo verrà considerato comunque valido. Esiste inoltre un'opzione globale situata in Opzioni472 che determina anche l'interrogazione degli host di Condivisione dominio66.

Nome host o IP

Immettere il nome host o l'indirizzo IP del server LDAP/Active Directory del dominio. MDaemon si connetterà a questo server LDAP/Active Directory per verificare la validità dell'indirizzo del destinatario di un messaggio in arrivo relativo al dominio per il quale MDaemon funge da gateway o da server di backup.

Porta

Specificare la porta utilizzata dal server LDAP/AD o Minger del dominio. MDaemon utilizzerà tale porta per la verifica delle informazioni relative all'indirizzo mediante LDAP, Active Directory o Minger.

Verifica

Fare clic su questo pulsante per controllare che le impostazioni per la verifica in remoto dell'indirizzo siano configurate correttamente. MDaemon tenterà semplicemente di connettersi al server LDAP/AD indicato e ne verificherà la corrispondenza con le informazioni specificate.

Cache

Fare clic su questo pulsante per aprire il file cache di LDAP/Minger. È possibile attivare o disattivare la cache mediante Opzioni472.

Nome utente o DN associato

Inserire il nome utente o il DN dell'account con accesso di tipo amministrativo al server LDAP/AD del dominio, in modo che MDaemon possa verificare i destinatari dei messaggi in arrivo indirizzati al dominio per il quale agisce da gateway o da server di

backup. Questo è il DN che viene usato per l'autenticazione nel procedimento di associazione.

Password/segreto condiviso Minger
La password viene trasmessa al server LDAP/AD del dominio insieme al valore *Associa DN* ai fini dell'autenticazione. Se si utilizza un server Minger, questo valore rappresenta il segreto condiviso o la password.

DN voce di base
Rappresenta il DN (Distinguished Name), ossia il punto iniziale nella struttura DIT (Directory Information Tree) a partire dal quale MDaemon esegue la verifica dell'account all'interno del server LDAP/AD.

Filtro di ricerca
Rappresenta il filtro di ricerca LDAP/AD utilizzato per la verifica degli indirizzi mediante le ricerche LDAP. MDaemon imposta un filtro di ricerca predefinito, appropriato nella maggior parte dei casi.

Ambito di ricerca:

Rappresenta l'ambito, ossia la portata delle ricerche LDAP/AD.

Solo DN base
Scegliere questa opzione se si desidera limitare la ricerca al solo DN base indicato in precedenza. In questo modo, la ricerca nella struttura DIT non verrà eseguita oltre tale punto.

1 livello inferiore al DN base
Utilizzare questa opzione se si desidera estendere la ricerca LDAP/AD ad un livello inferiore al DN specificato.

DN base e tutti gli elementi figlio
Con questa opzione, l'ambito della ricerca viene esteso dal DN fornito a tutti i relativi figli, fino all'ultimo elemento figlio del DIT.

File verifica indirizzi
Fare clic su questo pulsante per aprire l'elenco degli indirizzi e-mail validi del gateway, denominato `GatewayUsers.dat`. Il file include l'elenco degli indirizzi considerati destinatari validi per i messaggi in arrivo indirizzati ai gateway di dominio. MDaemon utilizza questo elenco come ulteriore fonte di indirizzi validi, indipendentemente dall'opzione di verifica impostata. Se si utilizza l'opzione *File*, tuttavia, il file rappresenta il solo e unico metodo di verifica utilizzato.

Uso di più configurazioni per le interrogazioni relative alla verifica LDAP

È possibile specificare più configurazioni LDAP per i domini del gateway. Per specificare insiemi aggiuntivi di parametri LDAP, impostare il primo normalmente, quindi modificare il file `GATEWAYS.DAT` manualmente utilizzando Blocco note.

Il nuovo insieme di parametri deve essere creato in base al formato seguente:

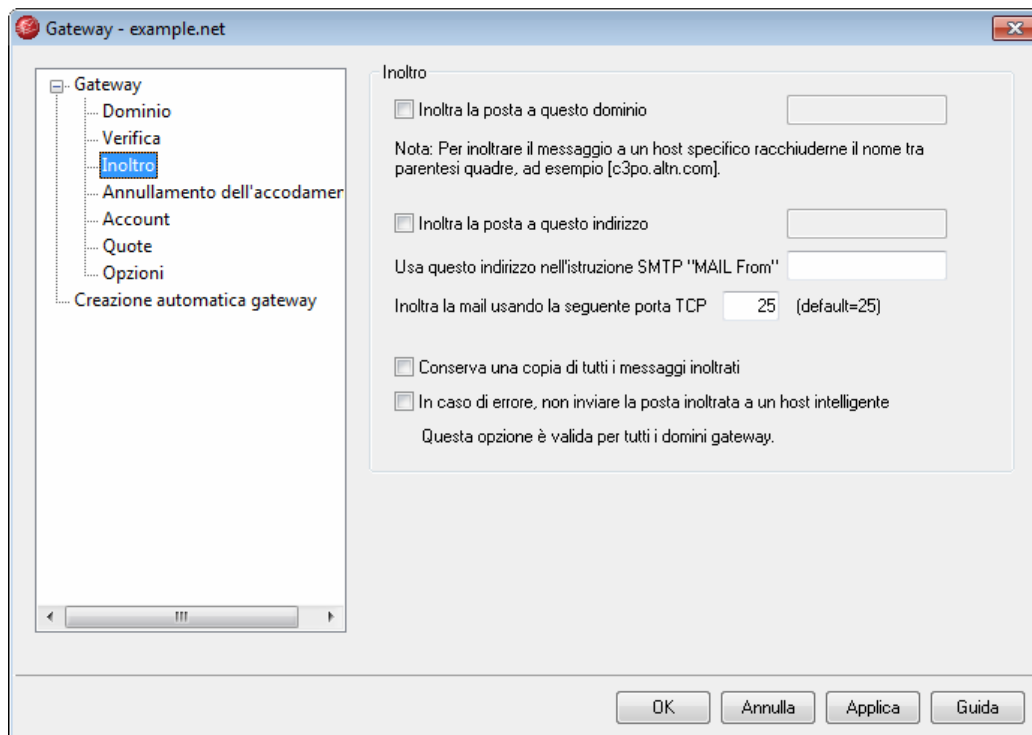
```
LDAPHost1=<nome host>
LDAPPort1=<porta>
LDAPBaseEntry1=<DN della voce di base>
LDAPRootDN1=<DN principale>
LDAPObjectClass1=USER
LDAPRootPass1=<password>
LDAPMailAttribute1=mail
```

Per ogni nuovo insieme di parametri, aumentare di 1 il valore numerale nel nome di ciascun parametro. Nell'esempio riportato in precedenza ogni nome di parametro termina con "1". Per creare un secondo insieme aggiuntivo, terminare ogni nome con "2". Per creare un terzo insieme, terminare ogni nome con "3" e così via.

Quando vengono eseguite le interrogazioni LDAP, MDaemon effettuerà più controlli in sequenza per individuare una corrispondenza. Se viene rilevata una corrispondenza oppure si verifica un errore, non verranno eseguiti ulteriori controlli.

Vedere:

Opzioni di LDAP e della rubrica 100
Minger 418

8.1.1.3 Inoltro

Inoltro

Inoltra la posta a questo dominio
In alcuni casi può essere conveniente inoltrare una copia di tutti i messaggi relativi a un dominio non appena questi arrivano. Se si desidera configurare MDaemon in questo modo, immettere il nome o l'indirizzo IP del dominio a cui devono essere inviate le copie della posta in arrivo. Se si desidera inoltrare i messaggi verso un host specifico, racchiuderne il nome tra parentesi quadre, ad esempio `[host1.esempio.com]`.

Inoltra posta all'indirizzo e-mail
Utilizzare questa funzione per inoltrare a un indirizzo e-mail specifico tutti i messaggi e-mail destinati al dominio client.

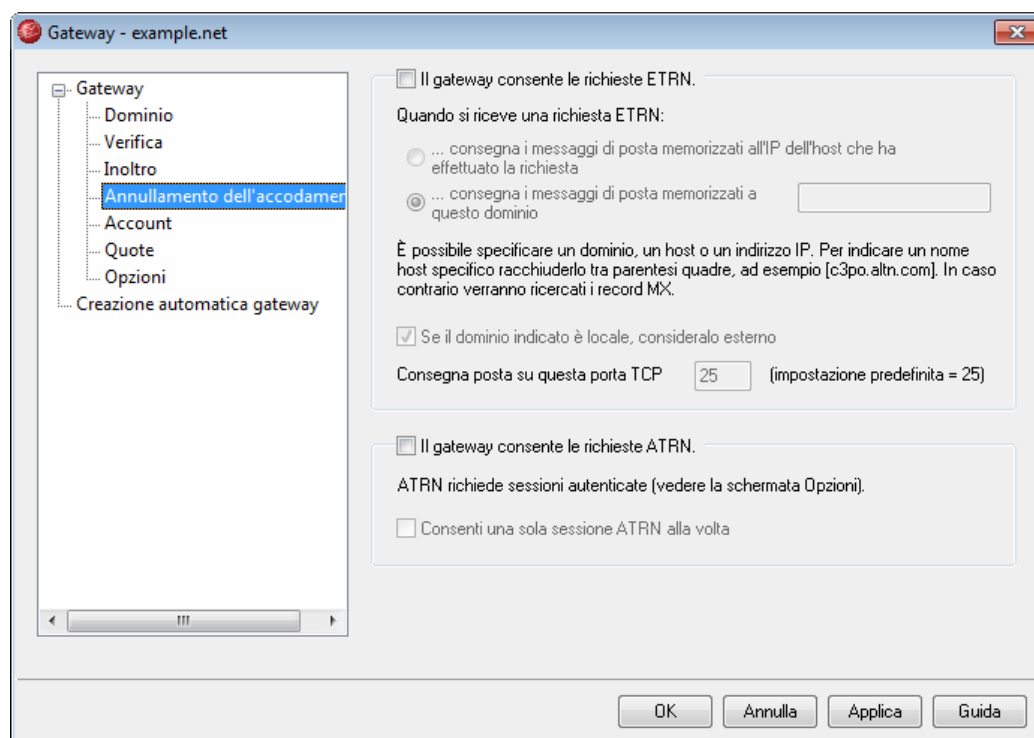
Usa questo indirizzo nell'istruzione SMTP "MAIL From"
MDaemon utilizzerà questo indirizzo nella transazione SMTP "Mail From".

Inoltra posta su questa porta TCP
MDaemon inoltrerà la posta mediante questa porta TCP.

Conserva una copia di tutti i messaggi inoltrati
Se si seleziona questa opzione, MDaemon conserverà una copia locale di ciascun messaggio inoltrato.

In caso di errore, non inviare la posta inoltrata a un host intelligente
Scegliere questa opzione per evitare l'invio di email inoltrate all'host specificato quando si verificano errori di consegna.

Si tratta di un'impostazione globale che viene applicata a tutti i gateway di dominio ed è disabilitata per impostazione predefinita.

8.1.1.4 Annullamento dell'accodamento

ETRN

Il gateway consente le richieste ETRN
Quando questa casella di controllo è abilitata, MDaemon risponde alle richieste ETRN effettuate da host qualificati per conto del dominio per cui MDaemon funge da gateway e-mail. Il comando ETRN è un'estensione SMTP che segnala al server nel quale è memorizzata la posta di un particolare dominio di iniziare lo spool. Quando MDaemon riceve una richiesta ETRN per un dominio, inizia immediatamente lo spool della posta memorizzata per la consegna mediante transazioni SMTP successive. La sessione SMTP che emette una richiesta ETRN non coincide con quella che riceve la posta memorizzata. Per inviare l'eventuale posta memorizzata per il dominio, MDaemon utilizza successive transazioni SMTP indipendenti. In questo modo, viene preservata la busta del messaggio e migliorato il livello di protezione. È opportuno tenere presente che l'host a cui MDaemon invia lo spool dell'eventuale posta

memorizzata potrebbe non iniziare immediatamente la ricezione dei messaggi. ETRN infatti garantisce solo che verrà effettuato lo *spool* di consegna per la posta memorizzata, ma il *processo* di consegna vero e proprio è soggetto ad altre limitazioni imposte dall'amministratore e potrebbe essere messo in attesa nella coda della posta in uscita fino all'esecuzione del successivo evento pianificato di elaborazione della posta remota. A causa di queste limitazioni, si consiglia di utilizzare il metodo ODMR (On-Demand Mail Relay) 60 e il relativo comando ATRN anziché ETRN. Si tenga tuttavia presente che questo metodo non è supportato da tutti i client e server e risulta pertanto disponibile solo per i domini client che utilizzano un server compatibile. MDaemon supporta totalmente il metodo ODMR, sia sul lato client che sul lato server.

Per impostazione predefinita, MDaemon richiede all'host che esegue la connessione con una richiesta ETRN un'autenticazione preliminare tramite ESMTP AUTH, utilizzando il *nome di dominio* 460 e la *password AUTH gateway* 472 come credenziali di registrazione. Se non si desidera richiedere l'autenticazione, è possibile disattivare questa opzione nella scheda Opzioni 472 deselezionando l'opzione *L'annullamento dell'accodamento dei messaggi ETRN richiede l'autenticazione*.

Quando si riceve una richiesta ETRN:

... consegna i messaggi di posta memorizzati all'IP dell'host che ha effettuato la richiesta
Quando questa opzione è selezionata, MDaemon invia l'eventuale posta archiviata all'indirizzo IP del computer da cui proviene la richiesta ETRN. Affinché i messaggi possano essere ricevuti, sul sistema richiedente deve essere in esecuzione un server SMTP.

... consegna i messaggi di posta memorizzati a questo dominio
Indica il nome dell'host, il nome di dominio o l'indirizzo IP a cui viene inviata l'eventuale posta memorizzata quando una richiesta ETRN viene ricevuta e soddisfatta. Affinché i messaggi possano essere ricevuti, nel sistema ricevente deve essere in esecuzione un server SMTP. Nota: se in questo campo viene specificato il nome di un dominio, è possibile utilizzare i record A e MX a seconda dei risultati DNS ottenuti durante la consegna. Se si desidera consegnare i messaggi a un host specifico racchiuderne il nome tra parentesi quadre (ad esempio, `[host1.esempio.net]`) oppure specificare un indirizzo IP anziché un nome di dominio.

Se il dominio indicato è locale, consideralo esterno
Attivare questo comando se il dominio è locale ma si desidera che lo spool della posta venga effettuato come se il dominio fosse remoto.

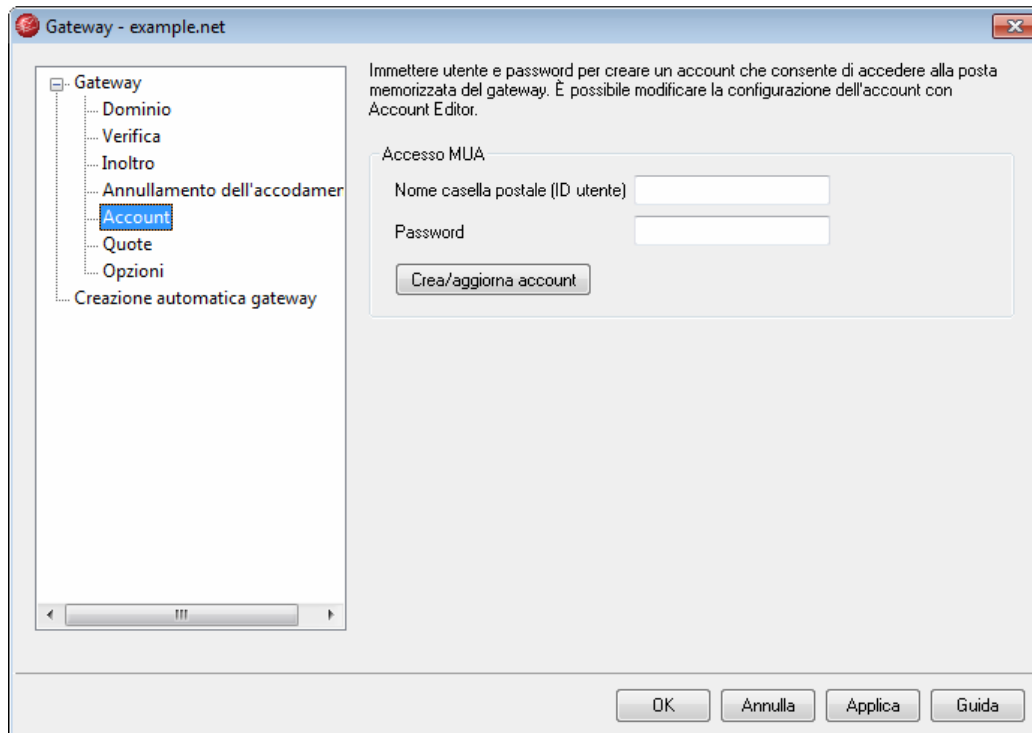
Consegna posta su questa porta TCP
Utilizzare questa casella per specificare la porta su cui deve essere effettuato lo spool della posta del dominio.

ATRN

Il gateway risponde alle richieste ATRN.
Abilitare questa opzione se si desidera che MDaemon risponda a comandi `ATRN` provenienti dal dominio del gateway. `ATRN` è un comando ESMTP utilizzato nel metodo ODMR (On-Demand Mail Relay) 60 e rappresenta il miglior metodo di inoltro finora disponibile per l'hosting della posta. ATRN rappresenta una soluzione da preferire a ETRN e ad altri metodi perché richiede l'autenticazione prima che venga annullato l'accodamento della posta, ma non un indirizzo IP statico. Quest'ultimo risulta superfluo perché il flusso di dati tra MDaemon e il dominio client viene invertito immediatamente e, diversamente da `ETRN` che utilizza una connessione separata una volta inviato il comando `ETRN`, lo spool dei messaggi viene annullato senza che debba essere stabilita una nuova connessione. In questo modo, i domini client che utilizzano un indirizzo IP dinamico (non statico) possono raccogliere i messaggi senza utilizzare POP3 o DomainPOP, in quanto la busta SMTP originale viene preservata.

ATRN richiede una sessione autenticata mediante AUTH. È possibile configurare le credenziali di autenticazione nella scheda Opzioni 472.

Consenti solo una sessione ATRN per volta
Fare clic su questa casella di controllo se si desidera limitare ATRN ad una sessione per volta.

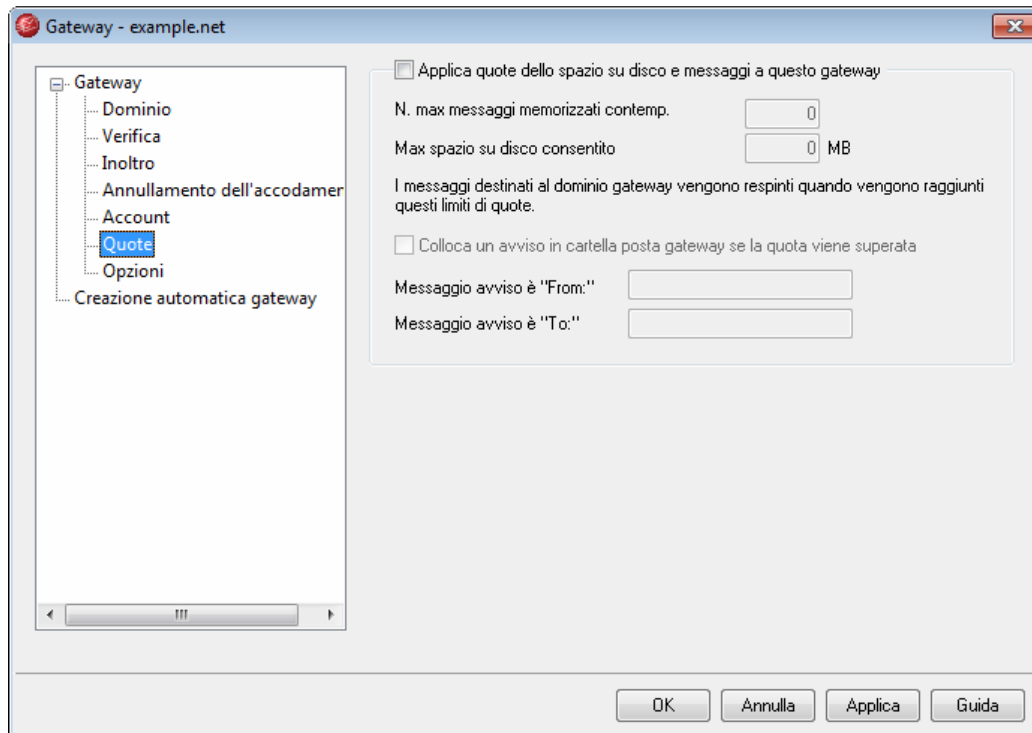
8.1.1.5 Account

Questa schermata consente di creare un account di MDaemon da associare con il gateway. Questo account consente ai server e-mail o ai client di posta di connettersi con MDaemon per raccogliere i messaggi del gateway tramite IMAP, DomainPOP o POP3. IMAP è disponibile solo in MDaemon PRO.

Nome casella postale (ID utente)
Inserire il nome della casella postale, ad esempio il nome dell'account utente, utilizzato dal client per accedere ai messaggi del gateway memorizzati nella relativa casella postale.

Password
Inserire la password utilizzata dal dominio client per accedere ai messaggi memorizzati nella relativa casella postale.

Crea/aggiorna account
Fare clic su questo pulsante per creare un account o per aggiornare il nome della casella postale e i valori relativi alla password, se l'account è già presente.

Account Manager 340 consente di modificare e di rimuovere un account. Prestare attenzione quando si desidera rimuovere un account perché, in questo, modo si eliminano anche la relativa posta e le cartelle, utilizzate anche dal gateway.

8.1.1.6 Quote

Quote

Applica quote dello spazio su disco e messaggi a questo gateway
Abilitare questa opzione se si desidera specificare il numero massimo di messaggi consentiti per il dominio e la quantità massima di spazio su disco (in kilobyte) utilizzabile, inclusi gli allegati di file codificati che si trovano nella directory Files. Quando la quota viene raggiunta, tutti i messaggi indirizzati al dominio vengono respinti.

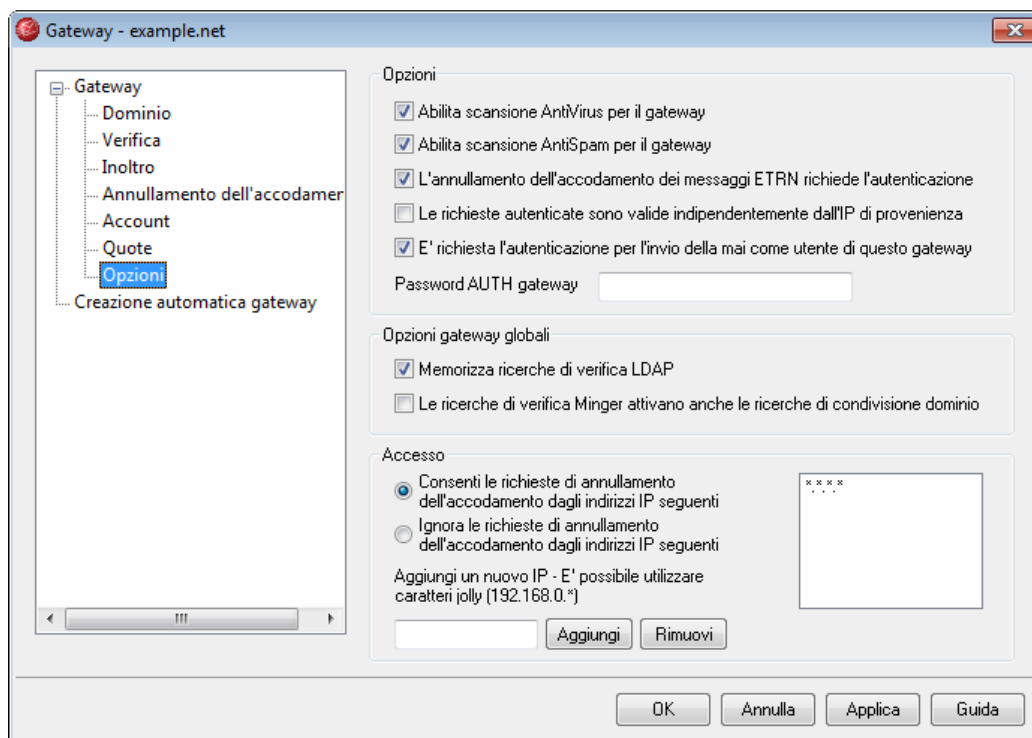
Numero massimo di messaggi memorizzati contemporaneamente
Questa casella consente di specificare il numero massimo di messaggi memorizzati per il dominio gateway. Specificare "0" in questa opzione se non si desidera inserire alcuna limitazione di dimensione.

Massimo spazio su disco consentito
Consente di specificare il limite massimo consentito per lo spazio su disco. Se la dimensione dei messaggi memorizzati raggiunge questo limite, tutti i messaggi indirizzati al dominio vengono respinti. Inserire "0" se non si desidera limitare il numero di connessioni simultanee.

Colloca un avviso in cartella posta gateway se la quota viene superata
Se questa opzione è abilitata e si tenta di consegnare all'account una quantità di posta superiore ai limiti stabiliti per i messaggi e lo spazio su disco, nella directory di posta del gateway di dominio viene collocato un avviso appropriato. Nei campi seguenti è possibile specificare le intestazioni "`From:`" e "`To:`" del messaggio di avviso.

Messaggio avviso è "From:"
Questa opzione consente di specificare l'indirizzo "From:" utilizzato nei messaggi di avviso relativi al superamento della quota.

Messaggio avviso è "To:"
Questa opzione consente di specificare l'indirizzo "To:" utilizzato nei messaggi di avviso relativi al superamento della quota.

8.1.1.7 Opzioni

Opzioni

Abilita scansione AntiVirus per il gateway
Selezionare questa opzione se si è installato SecurityPlus per MDaemon e si desidera eseguire la scansione dei messaggi del gateway di dominio. Se l'opzione è deselezionata, la scansione non viene eseguita.

Abilita scansione AntiSpam per il gateway
Scegliere questa opzione per applicare le impostazioni di Spam Filter ai messaggi del gateway di dominio. In caso contrario, Spam Filter non eseguirà la scansione dei messaggi.

L'annullamento dell'accodamento dei messaggi ETRN richiede l'autenticazione
Dopo aver configurato le impostazioni nella scheda Annullamento dell'accodamento in modo che vengano accettate le richieste ESMTP ETRN, per impostazione predefinita

viene utilizzata questa opzione che richiede all'host che esegue la connessione un'autenticazione preliminare mediante il comando ESMTP AUTH. Quando questa opzione è attivata, è necessario indicare una password di autenticazione nella casella "Password AUTH gateway" indicata di seguito.

Deselezionare questa casella di controllo se non si desidera richiedere l'autenticazione di host tramite richieste ETRN.

Le richieste autenticate sono valide indipendentemente dall'IP di provenienza
Selezionare questa casella di controllo se si desidera soddisfare le richieste autenticate a prescindere dall'indirizzo IP da cui provengono. Se questa opzione non è abilitata, potranno essere soddisfatte solo le richieste provenienti dagli indirizzi IP specificati nella sezione Accesso.

È richiesta l'autenticazione per l'invio della mail come utente di questo gateway
Selezionare questa casella di controllo se si desidera che per tutti i messaggi che affermano di appartenere al dominio venga richiesta l'autenticazione. Perché un messaggio venga considerato proveniente da questo dominio deve utilizzare una connessione autenticata (o collegarsi da un indirizzo IP accreditato), in caso contrario viene rifiutato. L'opzione è abilitata per impostazione predefinita.

Alla creazione di nuovi gateway di dominio, questa opzione viene attivata per impostazione predefinita. Se si desidera modificare le impostazioni predefinite in modo da disabilitare questa opzione per i nuovi gateway, modificare la seguente chiave nel file `MDaemon.ini`:

`[Special]`
`GatewaySendersMustAuth=No` (il valore predefinito è `Yes`)

Password AUTH gateway
Indicare la password AUTH del gateway in questo campo, quando si usa ATRN per annullare l'accodamento della posta del gateway o quando si richiede l'autenticazione tramite l'opzione *L'annullamento dell'accodamento ETRN richiede l'autenticazione*.

Il dominio per cui MDaemon funge da gateway e-mail deve utilizzare come parametro di accesso il proprio nome di dominio. Ad esempio, se il gateway di dominio è "esempio.com" e si sta utilizzando ATRN per annullare l'accodamento della relativa posta, l'autenticazione verrà effettuata tramite le credenziali di registrazione "esempio.com" e la password specificata in questo campo.

Opzioni gateway globali

Le opzioni seguenti sono opzioni globali e non sono limitate solo a questo dominio.

Memorizza ricerche di verifica LDAP
Selezionare questa casella di controllo se si desidera inserire nella cache i risultati delle ricerche di verifica 462 LDAP per i gateway di dominio.

Le ricerche di verifica Minger attivano anche le ricerche di condivisione dominio
Se si abilita questa opzione e uno dei gateway esegue la verifica degli indirizzi mediante Minger, oltre a interrogare l'host Minger indicato nella schermata Verifica 462, MDaemon interroga anche gli host di Condivisione dominio 66. Questa opzione è globale, ossia si applica a tutti i gateway impostati per eseguire la verifica degli indirizzi mediante Minger.

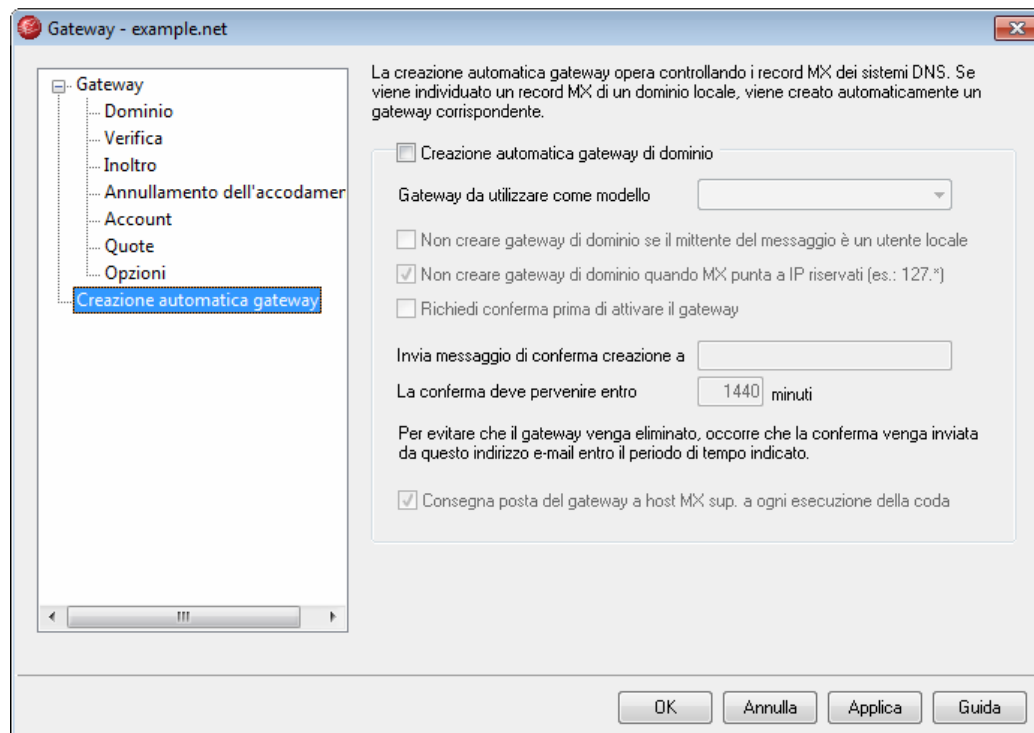
Accesso

Consenti le richieste di annullamento dell'accodamento dagli indirizzi IP seguenti
Quando questa opzione è selezionata, MDaemon soddisfa ogni richiesta ETRN/ATRN effettuata da un IP presente nell'elenco indirizzi associato.

Ignora le richieste di annullamento dell'accodamento dagli indirizzi IP seguenti
Quando questa opzione è selezionata, MDaemon ignora tutte le richieste ETRN/ATRN effettuate da un IP presente nell'elenco indirizzi associato.

Aggiungi
Per aggiungere un nuovo indirizzo IP all'elenco corrente, è sufficiente inserirlo nella casella di testo e fare clic sul pulsante *Aggiungi*.

Rimuovi
Fare clic su questo pulsante per rimuovere una voce selezionata dall'elenco degli indirizzi IP.

8.1.2 Creazione automatica di gateway

Creazione automatica di gateway (solo MDaemon PRO)

Questa funzionalità consente la creazione automatica di un Gateway di dominio 458 relativo a un dominio sconosciuto nel caso in cui un'altra origine tenti di consegnare a MDaemon i messaggi di tale dominio e il risultato di una query DNS indichi la posizione di MDaemon come record MX valido.

Ad esempio:

Si supponga di aver abilitato la creazione automatica di un dominio e che l'indirizzo IP del dominio predefinito di MDaemon sia `1.2.3.4`. Quando MDaemon riceve un messaggio via SMTP destinato al dominio sconosciuto `esempio.com`, esso ricerca i record MX e A del dominio `esempio.com` per verificare se il proprio indirizzo IP (`1.2.3.4`) è un host di inoltro della posta conosciuto: se i risultati delle interrogazioni DNS confermano che l'indirizzo IP di MDaemon è un host MX valido per `esempio.com`, MDaemon crea automaticamente un nuovo gateway di dominio e ne accetta la posta. I messaggi indirizzati a `esempio.com` vengono archiviati in una cartella speciale e, se necessario, accodati in host MX di livello superiore a ogni intervallo di elaborazione della posta remota. Questa funzione trasforma di fatto il server in un server di backup per un altro dominio, semplicemente configurando il sistema DNS in modo che utilizzi l'indirizzo IP del server come host MX alternativo.

Per garantire la sicurezza di questa funzione, è possibile configurare MDaemon in modo da inviare una richiesta di conferma a un indirizzo e-mail desiderato. Durante l'attesa della conferma, i messaggi per il dominio vengono accettati e memorizzati, ma non consegnati. Le richieste di conferma devono avere riscontro entro un tempo specificato. In caso contrario, il gateway creato automaticamente verrà rimosso e tutti

i messaggi archiviati verranno cancellati. Se la conferma viene ricevuta entro il tempo previsto, i messaggi archiviati verranno consegnati normalmente.

È possibile che un utente malintenzionato o "spammer" tenti di sfruttare questa funzione configurando il proprio server DNS in modo che l'indirizzo IP di MDaemon figuri come host MX. La funzione Creazione automatica di gateway deve essere usata con la massima cautela. Per prevenire eventi indesiderati, si consiglia di utilizzare sempre, se possibile, il comando *Invia messaggio di conferma della creazione a*.

Creazione automatica gateway di dominio
Fare clic su questa casella di controllo se si desidera che i gateway di dominio vengano creati automaticamente in base ai risultati delle interrogazioni DNS.

Gateway da utilizzare come modello
Scegliere un gateway di dominio dall'elenco a discesa per utilizzarne le impostazioni come modello per tutti i gateway che verranno creati automaticamente.

Non creare gateway di dominio se il mittente del messaggio è un utente locale
Abilitare questa opzione per evitare che i messaggi provenienti da utenti locali possano avviare la creazione automatica di gateway.

Non creare gateway di dominio quando MX punta a IP riservati
Selezionare questa casella di controllo per impedire la creazione di un gateway automatico se il record MX punta a un indirizzo IP riservato, ad esempio 127.*, 192.* o simili.

Richiedi conferma prima di attivare il gateway
Se questa opzione è abilitata, MDaemon invia una conferma all'indirizzo e-mail desiderato per determinare se il gateway creato automaticamente è valido. Nonostante continui da accettare i messaggi per il dominio in questione, MDaemon non effettua la consegna finché non viene ricevuta la conferma.

Invia messaggio di conferma creazione a
Immettere l'indirizzo a cui inviare i messaggi di conferma in questa casella di testo.

La conferma deve pervenire entro XX minuti
Immettere il numero di minuti per cui MDaemon attende la conferma. Alla scadenza di questo limite di tempo, il gateway di dominio viene eliminato.

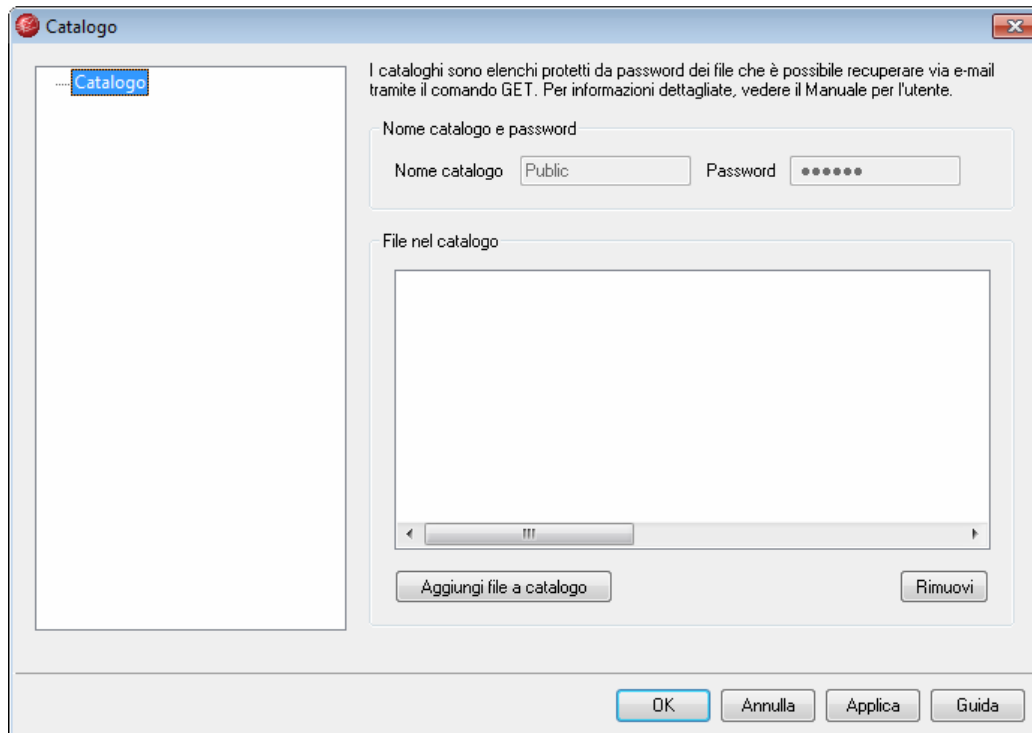
Consegna posta del gateway a host MX superiori a ogni esecuzione della coda
Abilitare questa opzione per specificare che a ogni elaborazione della coda remota i messaggi di questo gateway devono essere consegnati a host MX superiori.

Per ulteriori informazioni, vedere

Gateway di dominio 458
Gateway Editor 459

Sezione IX

9 Menu Cataloghi

9.1 Editor cataloghi

Selezionare Cataloghi » Nuovo catalogo o Cataloghi » Modifica catalogo per aprire l'editor dei cataloghi che consente di creare o modificare i cataloghi di file. I cataloghi possono essere utilizzati per richiedere file presenti sulla rete e riceverli via e-mail in formato codificato e consentono all'amministratore dei servizi di posta di assegnare "nomi magici", ovvero scorciatoie, ai file archiviati su disco. Analogamente agli alias, i nomi magici puntano a uno specifico file che si trova in una posizione accessibile a MDaemon. L'utente può utilizzare un tipo speciale di messaggio e-mail per richiedere il file mediante il nome magico. Il formato del messaggio e-mail speciale è descritto nella sezione Controllo remoto del server 506 (vedere il comando **GET** in Controllo delle liste di distribuzione e dei cataloghi 508.

Nome catalogo e password

Nome catalogo
Immettere il nome del catalogo file in questo campo.

Password
Immettere la password del catalogo file in questo campo.

Le password relative ai cataloghi non sono obbligatorie. È infatti possibile scegliere di rendere i cataloghi accessibili anche senza password.

Per ulteriori informazioni, vedere

Controllo dei cataloghi e delle liste di distribuzione 508

File nel catalogo

In questa finestra vengono visualizzati i file e i corrispondenti "nomi magici" attualmente associati al catalogo specificato. Fare doppio clic su una voce visualizzata in questa finestra per rimuoverla dal catalogo.

Rimuovi
Fare clic su questo pulsante per rimuovere una voce selezionata dall'elenco dei file.

Aggiungi file a catalogo
Fare clic su questo pulsante per aggiungere un file al catalogo. Una volta selezionato il file da aggiungere, verrà chiesto di indicare il *Nome magico* che si desidera assegnare al file. Scegliendo OK, il file e il nome magico a esso associato verranno aggiunti all'elenco.

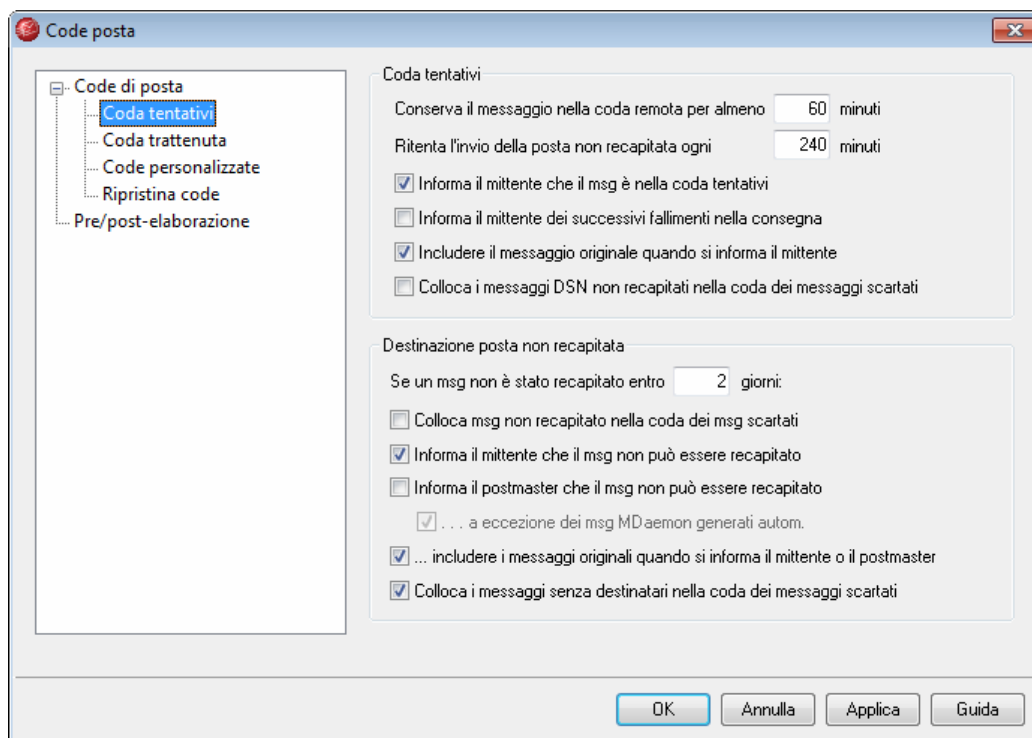
Il catalogo PUBLIC

Il catalogo PUBLIC rappresenta un'eccezione alle normali regole per l'accesso ai cataloghi di file. Per accedere a un catalogo, è solitamente necessario specificare la password precedentemente assegnata. Per il catalogo PUBLIC, la password non è obbligatoria. I file presenti nel catalogo PUBLIC sono disponibili a chiunque conosca il nome magico del file.

Sezione X

10 Menu Code posta

10.1 Code posta

10.1.1 Coda tentativi

La finestra di dialogo Coda tentativi, situata in Code posta » Code posta, consente di indicare a MDaemon come gestire i messaggi che non può consegnare a causa di errori reversibili, ad esempio quando il server ricevente è temporaneamente non disponibile.

Coda tentativi

Conserva il msg nella coda remota per almeno XX minuti
In questo campo si specifica quanto tempo un messaggio deve rimanere nella coda remota prima di essere rimosso e collocato nella coda tentativi. In genere, la coda remota è impostata per tentare di inviare i messaggi più frequentemente rispetto alla coda tentativi.

Ritenta l'invio della posta non recapitata ogni XX minuti
Questa impostazione definisce la frequenza con cui vengono elaborati i messaggi presenti nella coda tentativi.

Informa il mittente che il msg è nella coda tentativi
Selezionando questa casella, si informa il mittente che il messaggio è stato rimosso e collocato nella coda tentativi. È possibile trovare (e modificare) il testo di questo messaggio all'interno del file `DeliveryWarning.dat` della cartella `\app\` di MDaemon.

Informa il mittente dei successivi fallimenti nella consegna
Se la consegna di un messaggio presente nella coda tentativi non riesce, il mittente ne riceve notifica. È possibile trovare (e modificare) il testo di questo messaggio all'interno del file `DeliveryWarning.dat` della cartella `\app\` di MDaemon.

Includere il messaggio originale quando si informa il mittente
Selezionare questa opzione se si desidera allegare il messaggio originale a quello di notifica.

Colloca i messaggi DSN non recapitati nella coda dei messaggi scartati
Selezionare questa casella di controllo se si desidera collocare i messaggi DSN (Delivery Status Notification, Notifica dello stato del recapito) nella coda messaggi scartati anziché tentarne il reinvio.

Questa impostazione viene applicata solo ai messaggi DSN generati da MDaemon.

Destinazione posta non recapitata

Se un msg non è stato recapitato entro XX giorni
Questa impostazione determina per quanti giorni un messaggio può rimanere nella coda tentativi prima di essere rimosso. Se si inserisce "0", il messaggio verrà rispedito al mittente dopo il primo tentativo di reinvio. L'impostazione predefinita è 2 giorni.

Colloca msg non recapitato nella coda dei msg scartati
Quando si abilita questa opzione, il messaggio viene spostato nella coda dei messaggi scartati ogni volta che si raggiunge il limite impostato nell'opzione "*Se un messaggio non è stato recapitato entro XX giorni*"

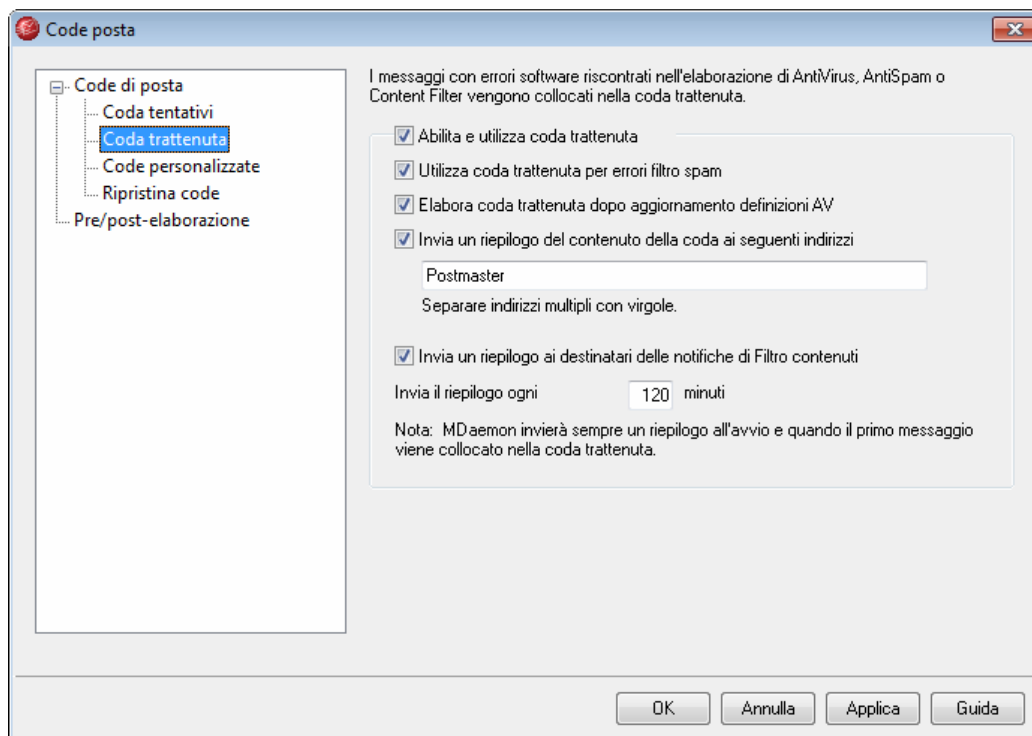
Informa il mittente che il msg non può essere recapitato
Quando per un messaggio sia stato raggiunto il limite impostato nell'opzione "*Se un msg non è stato recapitato entro XX giorni*", abilitando questa opzione MDaemon invia al mittente un messaggio per informarlo che il messaggio è stato rimosso definitivamente dal server. È possibile trovare (e modificare) il testo di questo messaggio all'interno del file `DeliveryError.dat`.

Informa il postmaster che il msg non può essere recapitato
Se questa casella è selezionata, viene inviato al postmaster un avviso in cui si indica che un messaggio è stato eliminato in maniera definitiva dal sistema tentativi.

... a eccezione dei messaggi MDaemon generati automaticamente
Per impostazione predefinita, il sistema tentativi non informa il postmaster dell'impossibilità di consegnare un messaggio generato automaticamente da MDaemon. Per informare il postmaster anche del mancato recapito di questi messaggi, abilitare questa casella di controllo. Le notifiche di ricevuta di ritorno, i messaggi creati come risposte automatiche e i risultati delle elaborazioni applicate agli account sono esempi di messaggi generati automaticamente.

...includere i messaggi originali quando si informa il mittente o il postmaster
Selezionare questa opzione se si desidera allegare il messaggio originale a quello inviato al mittente o al postmaster per segnalare la consegna non riuscita.

Colloca i messaggi senza destinatari nella coda dei messaggi scartati
Se questa opzione è abilitata, i messaggi senza l'indicazione del destinatario vengono collocati nella coda dei messaggi scartati. Se questa opzione è disabilitata, vengono eliminati. L'opzione è abilitata per impostazione predefinita.

10.1.2 Coda trattenuta

La coda trattenuta, disponibile in `Code posta » Code posta`, può essere utilizzata per ricevere i messaggi che hanno determinato eccezioni software durante l'elaborazione di AntiVirus, AntiSpam o Filtro contenuti. Qualora si verifichi un errore software durante l'elaborazione di un messaggio, questo viene spostato nella coda trattenuta senza essere consegnato.

I messaggi collocati nella coda trattenuta vi rimangono finché l'amministratore non li rimuove. L'opzione *Elabora coda trattenuta* è presente sia nella barra degli strumenti di MDaemon sia nella barra di menu `Code posta`. È possibile elaborare i messaggi anche facendo clic con il pulsante destro del mouse sulla coda trattenuta nell'interfaccia principale e scegliendo la voce "Riaccoda" dal menu di scelta rapida. L'elaborazione della coda trattenuta sposta tutti i messaggi nella coda remota o locale per la normale elaborazione della posta. Se l'errore che ha determinato l'inserimento del messaggio nella coda trattenuta si verifica ancora, il messaggio viene reinserito nuovamente nella coda trattenuta. Se si desidera tentare di consegnare i messaggi della coda trattenuta ignorando eventuali errori, fare clic con il pulsante destro del mouse sulla coda trattenuta dell'interfaccia principale e scegliere dal menu la voce "Rilascia". Quando

vengono rilasciati messaggi dalla coda trattenuta, appare un avviso sulla possibilità che alcuni messaggi contengano virus o non siano gestiti dai moduli di Filtro contenuti, AntiSpam e/o AntiVirus.

Coda trattenuta

Abilita e utilizza coda trattenuta
Per attivare la coda trattenuta, selezionare questa casella di controllo. I messaggi che hanno determinato eccezioni software durante l'elaborazione di AntiVirus e Filtro contenuti verranno spostati in questa coda qualora si verifichi un errore.

Utilizza coda trattenuta per errori filtro spam
Fare clic su questa opzione se si desidera spostare nella coda trattenuta i messaggi che determinano errori durante l'elaborazione di Spam Filter.

Elabora coda trattenuta dopo aggiornamento definizioni AV
Se si abilita questa opzione, la coda trattenuta viene elaborata automaticamente quando vengono aggiornate le definizioni dei virus di SecurityPlus per MDaemon 211.

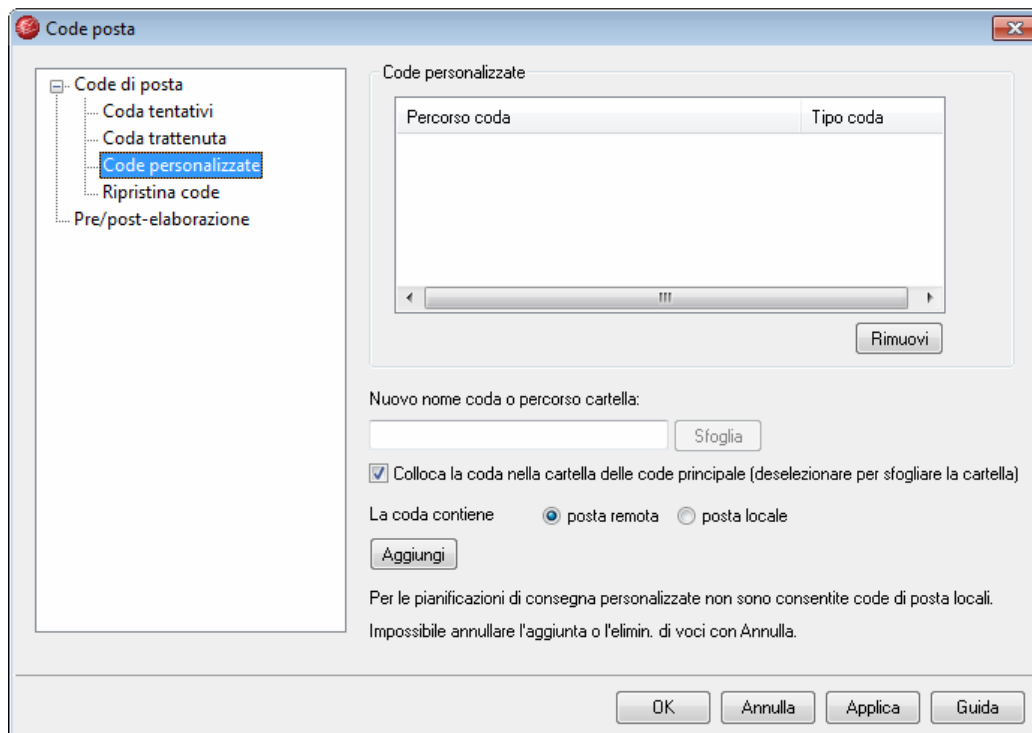
Invia un riepilogo del contenuto della coda ai seguenti indirizzi
Se si desidera inviare un riepilogo dei messaggi contenuti nella coda trattenuta a uno o più indirizzi e-mail a intervalli regolari, fare clic su questa opzione ed elencare gli indirizzi nell'apposito campo. Nel caso in cui si elencano più indirizzi, separarli con una virgola.

I messaggi di notifica vengono inviati all'avvio di MDaemon, al primo inserimento di un messaggio nella coda trattenuta e, successivamente, a intervalli regolari (specificati nell'opzione *Invia il riepilogo ogni XX minuti*).

Se il messaggio di notifica genera errori software, non viene consegnato ai destinatari remoti, ma solo ai destinatari locali..

Invia un riepilogo ai destinatari delle notifiche di Filtro contenuti
Fare clic su questa opzione se si desidera che una copia aggiuntiva di ciascun messaggio di notifica venga inviata ai destinatari 229 specificati per le notifiche di Filtro contenuti.

Invia il riepilogo ogni XX minuti
Scegliere questa opzione per specificare il numero di minuti che devono passare prima che MDaemon invii un messaggio di notifica della coda trattenuta agli indirizzi specificati o ai destinatari delle notifiche di Filtro contenuti.

10.1.3 Code personalizzate

La finestra di dialogo Code personalizzate, disponibile in Code posta » Code posta, consente di creare code di posta locali e remote personalizzate. Il supporto per le code personalizzate consente di monitorare diverse posizioni da cui inviare la posta. È possibile creare nuove code sia locali sia remote e utilizzare le funzioni di Filtro contenuti per collocare automaticamente i messaggi nelle code di posta personalizzate. Nel caso di code di posta remote, è possibile utilizzare Pianificazione eventi 156 per creare pianificazioni personalizzate al fine di controllare la frequenza di elaborazione di tali code.

Code personalizzate

Questa area include una voce per ciascuna coda personalizzata che consente di visualizzare il percorso del file associato alla coda e la tipologia di coda (locale o remota).

Rimuovi
Per rimuovere una coda dall'elenco, selezionarla e fare clic sul pulsante *Rimuovi*.

Se si elimina una coda personalizzata, verranno eliminate anche le pianificazioni personalizzate e le regole di Filtro contenuti associate alla coda.

Nuovo nome coda o percorso cartella
Specificare in questo campo di testo il nome della coda o il percorso della cartella da utilizzare come coda di posta. Se si desidera inserire il percorso completo di un file o

individuare una cartella specifica, deselezionare l'opzione "*Colloca la coda nella cartella delle code principale (deselezionare per sfogliare la cartella)*". Se l'opzione è selezionata, la coda verrà creata all'interno della cartella `\queues\` di MDaemon.

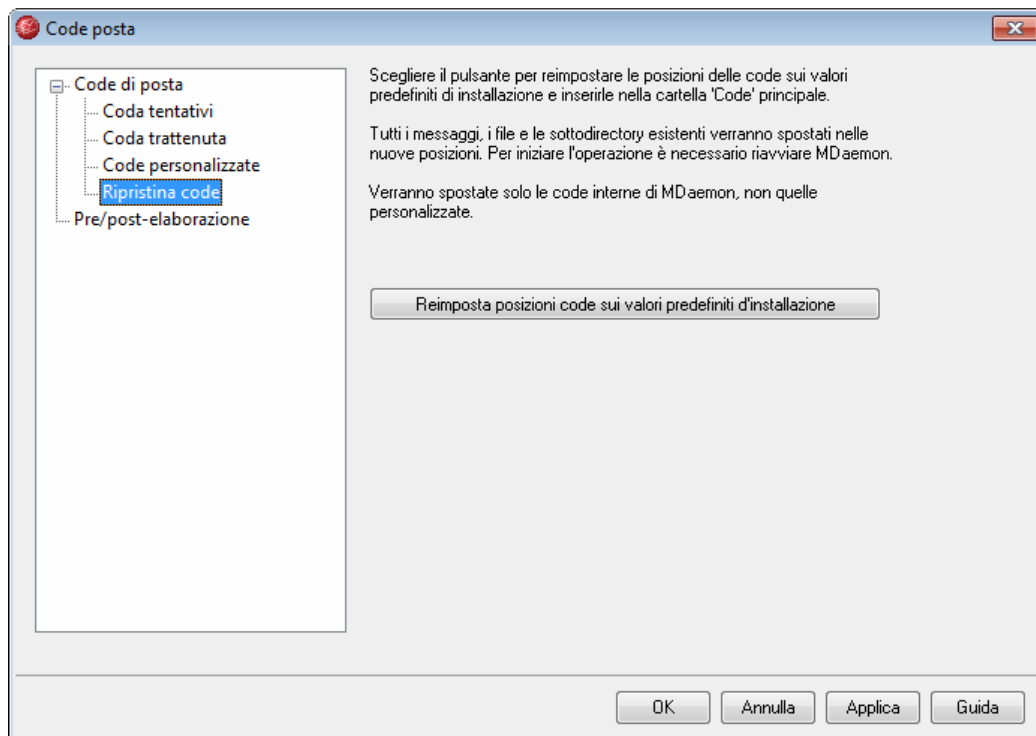
Colloca la coda nella cartella delle code principale (deselezionare per sfogliare la cartella)
Se questa casella di controllo è abilitata, il nome della coda specificato con l'opzione "*Nuovo nome coda o percorso cartella*" verrà creata come sottocartella della cartella `\queues\` di MDaemon. Se si disabilita questa casella di controllo, la sottocartella associata al nome coda specificato verrà creata nella cartella `\app\` di MDaemon. Se questa opzione è disabilitata, è possibile digitare il percorso file completo oppure utilizzare il pulsante Sfoglia per selezionare manualmente la cartella da utilizzare come coda personalizzata.

La coda contiene

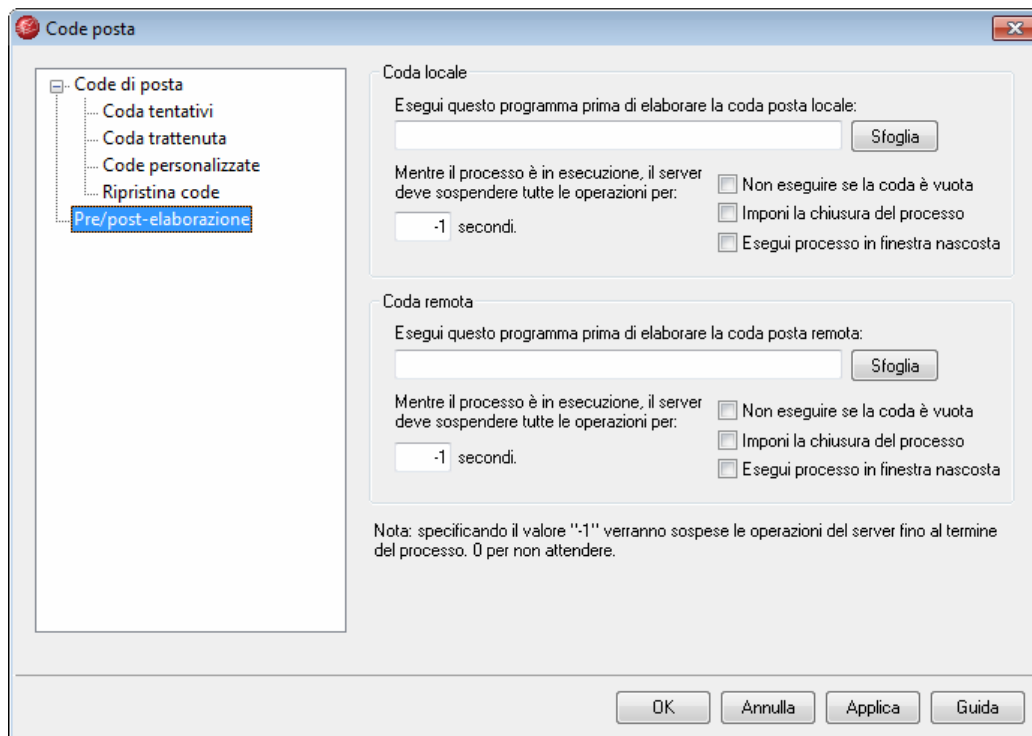
posta remota
Selezionare questa opzione per utilizzare la coda personalizzata per la posta remota.

posta locale
Selezionare questa opzione per utilizzare la coda personalizzata per la posta locale.

Aggiungi
Dopo avere indicato il nome, la posizione e il tipo della nuova coda, fare clic sul pulsante *Aggiungi* per aggiungerla all'elenco delle code personalizzate.

10.1.4 Ripristina code

Reimposta posizioni code su valori predefiniti d'installazione
Per impostazione predefinita, le nuove installazioni di MDaemon prevedono l'archiviazione delle code dei messaggi, ad esempio la coda remota, le code locali, la coda RAW e così via, nella sottocartella `\MDaemon\Queues\`. Le precedenti versioni di MDaemon archiviano le code in cartelle differenti. Se l'installazione di MDaemon usa la precedente posizione delle cartelle ma si desidera spostare le code in questa nuova struttura meglio organizzata, fare clic su questo pulsante per spostare tutte le code, i file e i messaggi contenuti. Dopo aver fatto clic su questo pulsante, riavviare MDaemon per implementare le modifiche apportate.

Le code personalizzate 488 non verranno spostate.

10.2 Pre/post-elaborazione

Pre/post elaborazione delle code locali e remote

Esegui questo programma prima di elaborare la coda posta locale
In questo campo vengono specificati il percorso e il nome del programma che verrà eseguito subito prima di elaborare e consegnare qualsiasi messaggio in formato RFC-2822 presente nelle code dei messaggi locali o remote. Se non vengono inserite informazioni di percorso complete, MDaemon cerca l'eseguibile dapprima nella propria directory, quindi nella directory System di Windows, successivamente nella directory Windows e infine nelle directory elencate nella variabile ambientale PATH.

Mentre il processo è in esecuzione, il server deve sospendere tutte le operazioni per XX secondi
Il valore inserito in questo campo determina il comportamento di MDaemon durante l'esecuzione del programma specificato. MDaemon può essere configurato per interrompere momentaneamente il thread di esecuzione per l'intervallo di tempo (in secondi) specificato, in attesa del risultato dell'elaborazione. Se l'elaborazione si riattiva prima che sia trascorso l'intervallo di tempo specificato, MDaemon riprende immediatamente il thread di esecuzione. Specificando il valore "0", MDaemon non effettua alcuna pausa, mentre immettendo "-1" MDaemon attende la ripresa dell'elaborazione, indipendentemente dalla durata dell'attesa.

Non eseguire se la coda è vuota
Selezionare questa casella di controllo se non si desidera che il programma specificato venga eseguito quando la coda è vuota.

Imponi la chiusura del processo
In alcuni casi, il processo da eseguire potrebbe non chiudersi autonomamente. Se questa casella è selezionata, MDaemon impone la chiusura della sessione allo scadere del tempo specificato in *...sospendere tutte le operazioni per XX secondi*. Questo comando non ha alcun effetto se l'intervallo di tempo trascorso è impostato su "-1".

Esegui processo in finestra nascosta
Selezionare questa casella di controllo se si desidera che il processo venga eseguito in una finestra nascosta.

10.3 Gestione delle code e delle statistiche

Il modulo di gestione delle code e delle statistiche di MDaemon è disponibile nel menu Code posta » Gestione code e statistiche. Gestione code e statistiche è una finestra di dialogo composta da quattro schede, ognuna progettata per uno scopo preciso, con un formato intuitivo e di facile utilizzo.

Pagina code 493

La scheda predefinita è *Pagina code*, da cui è possibile accedere con facilità a tutte le code di posta standard di MDaemon nonché alle cartelle delle caselle postali degli account utente. Mediante un semplice clic sulla coda o sull'utente desiderato, è possibile visualizzare un elenco di tutti i file di messaggio contenuti nella coda specificata e alcune informazioni rilevanti su ogni messaggio, ad esempio il mittente, il destinatario, il contenuto dell'intestazione "Deliver-To", l'oggetto, le dimensioni e l'intervallo di tempo per cui il messaggio è rimasto nella posizione corrente. In questa pagina sono inoltre presenti i comandi che consentono di copiare o di spostare i messaggi in cartelle diverse, nonché di eliminarli in modo irreversibile.

Pagina utente 496

Nella *Pagina utente* viene visualizzato l'elenco di tutti gli utenti di MDaemon. Per ogni utente vengono riportati il nome completo, il nome della casella postale, il numero di messaggi presenti nella casella postale, la quantità di spazio su disco occupato e la data in cui è stato effettuato l'ultimo controllo della posta. L'elenco può anche essere salvato su disco come file di testo oppure in formato delimitato da virgole per l'utilizzo nei database.

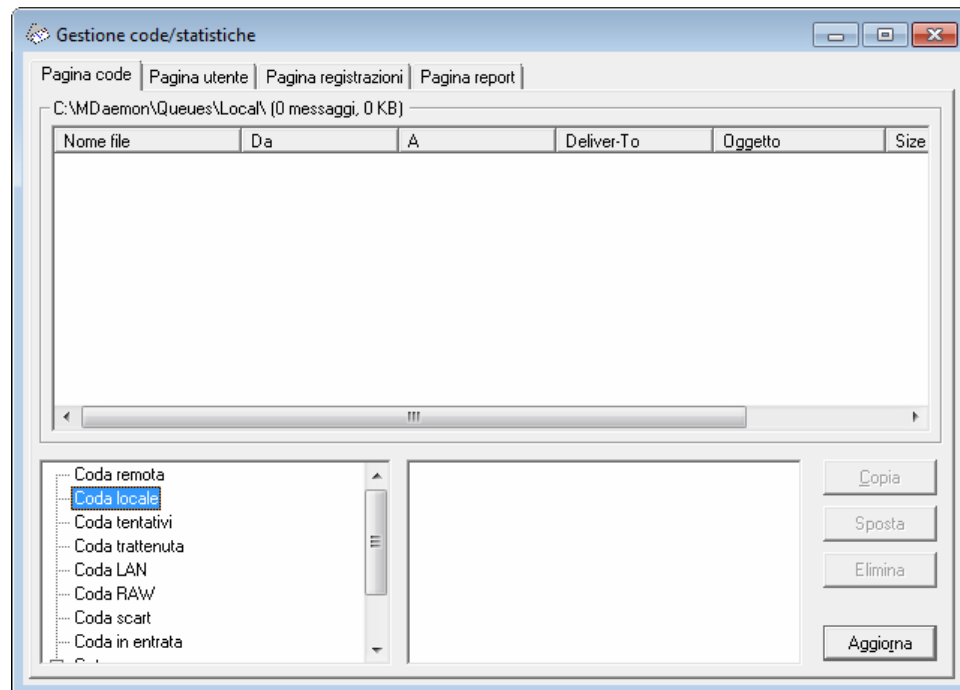
Pagina registrazioni 498

Questa finestra consente di visualizzare i *file registro* di MDaemon in formato elenco semplice. La funzione risulta utile per esaminare rapidamente la cronologia delle transazioni di posta di MDaemon, perché condensa il *file registro* selezionato in un elenco a colonne contenente il tipo di messaggio (POP in entrata, DomainPOP, RFC2822, e così via), l'host a cui si è connesso MDaemon durante la transazione, il mittente, il destinatario, le dimensioni del messaggio, la data di elaborazione di ciascun messaggio e l'esito della transazione. Per esaminare più dettagliatamente le voci del registro, è sufficiente fare doppio clic sulla voce desiderata. Verrà visualizzata la porzione di registro nella quale è stata eseguita la transazione. I registri visualizzati in *Pagina registrazioni* possono essere salvati come file di testo oppure in formato delimitato da

virgole per l'utilizzo nei database.

Pagina report 500

L'ultima scheda è *Pagina report*, che consente di creare un report contenente tutte le impostazioni di configurazione di MDaemon in formato leggibile (testo normale). In MDaemon è presente una grande quantità di impostazioni e configurazioni opzionali. Questa funzione consente di accelerare sensibilmente il processo di gestione delle modifiche apportate alla configurazione, nonché di facilitare la diagnosi dei possibili problemi. Inoltre, il report viene visualizzato in un formato di testo modificabile che consente di copiare e incollare le informazioni (mediante il menu di scelta rapida associato al clic con il pulsante destro del mouse) oppure di aggiungere annotazioni e altre specifiche prima di salvare il file.

10.3.1 Pagina code

Casella di riepilogo della pagina code

Quando si sceglie una coda o un utente dall'area *Code* o dalla casella di riepilogo degli utenti, nella casella di riepilogo principale di questa pagina viene visualizzato un elenco di tutti i file di messaggio contenuti nella coda selezionata. Per ogni messaggio, l'elenco contiene il nome del file, il mittente, il destinatario, il contenuto dell'intestazione "Deliver-To", l'oggetto, la dimensione e l'intervallo di tempo (data e ora) per cui è rimasto nella posizione corrente.

Nell'area soprastante questa casella viene riprodotto il percorso completo della directory correntemente visualizzata, nonché il numero dei messaggi visualizzati e la dimensione della directory stessa.

È possibile copiare, spostare o eliminare uno o più file selezionandoli dall'elenco, quindi facendo clic sul pulsante sottostante appropriato.

Il contenuto dei file può anche essere modificato direttamente dalla casella di riepilogo nella *Pagina code*. Se si fa doppio clic sul file da modificare oppure si sceglie "Modifica" dal menu di scelta rapido associato al clic del pulsante destro del mouse, il file verrà aperto in Blocco note di Windows per consentirne la modifica.

Se si desidera che, per impostazione predefinita, venga aperto un editor diverso da Blocco note, è necessario modificare il file `mdstats.ini` presente nella directory `\MDaemon\app\`. Modificare la chiave "`Editor=`" nella sezione `[QueueOptions]` in `Editor=EditorPersonale.exe`. Se il file `*.exe` non si trova nel percorso corrente, è necessario includere il percorso con il nome file.

È possibile spostarsi all'interno della casella di riepilogo mediante le barre di scorrimento verticale e orizzontale oppure facendo clic in qualunque punto della casella di riepilogo e utilizzando i tasti FRECCIA. È possibile ordinare le informazioni contenute nella casella di riepilogo *Pagina code* in base a qualunque colonna. Fare clic una volta sulla colonna desiderata per ordinarla in modo ascendente (A-Z, 1-2) oppure doppio clic per ordinarla in modo discendente (Z-A, 2-1). Le colonne possono inoltre essere ridimensionate posizionando il puntatore sulla linea che separa le intestazioni di colonna finché non cambia forma, quindi trascinando la colonna fino a raggiungere la dimensione desiderata.

Selezione dei file

Per selezionare singoli file — Fare clic sul file desiderato.

Per selezionare file adiacenti — Fare clic sul primo file del gruppo di file adiacenti che si desidera selezionare, quindi, tenendo premuto il tasto MAIUSC, fare clic sull'ultimo file del gruppo.

In alternativa, utilizzare i tasti FRECCIA, HOME, FINE, PAGSU e PAGGIÙ tenendo premuto il tasto MAIUSC.

Per selezionare file non adiacenti — Fare clic sui file desiderati nella colonna **Nome file** tenendo premuto il tasto CTRL.

Code dei messaggi

Fare clic su una voce nel riquadro inferiore sinistro per visualizzare nella casella di riepilogo *Pagina code* un elenco di tutti i file contenuti in una determinata coda. Se si fa clic sull'opzione *Cartelle utente*, nella casella di riepilogo degli *utenti* alla destra della sezione relativa alle *code dei messaggi* verrà visualizzato l'elenco di tutti gli utenti di MDaemon.

Casella di riepilogo degli utenti

In questa casella viene visualizzato un elenco di tutti gli utenti MDaemon quando si fa clic sull'opzione *Cartelle utente* all'interno della sezione relativa alle *code dei messaggi* nel riquadro inferiore sinistro. Fare clic sul nome di un utente per visualizzare un elenco di tutti i file messaggio correntemente contenuti nella cartella della casella

postale dell'utente.

Aggiorna
Poiché le code di posta vengono modificate dinamicamente mentre MDaemon è attivo grazie al trasferimento costante dei file di messaggio da e per le code, è opportuno fare regolarmente clic su questo pulsante per aggiornare l'elenco di file visualizzato.

È possibile modificare il file `MDstats.ini` in modo che gli elenchi visualizzati vengano aggiornati automaticamente. A questo scopo, è sufficiente aprire il file `MDstats.ini` presente nella directory `\app\` di MDaemon e modificare la chiave AutoRefresh in `[QueueOptions]` per farla corrispondere all'intervallo in secondi che deve trascorrere tra un aggiornamento e un altro. Se si specifica il valore "`0`", l'elenco non verrà aggiornato automaticamente. Esempio: `AutoRefresh=15` (l'elenco viene aggiornato ogni 15 secondi).

Copia
Fare clic su questo pulsante per copiare i file precedentemente selezionati nella cartella della casella postale di un'altra coda o di un altro utente. Una volta fatto clic sul pulsante, viene visualizzata la finestra di dialogo *Copia messaggi*, nella quale è possibile selezionare la posizione in cui si desidera copiare i file selezionati.

Sposta
Fare clic su questo pulsante per spostare i file precedentemente selezionati nella cartella della casella postale di un'altra coda o di un altro utente. Una volta fatto clic sul pulsante, viene visualizzata la finestra di dialogo *Sposta messaggi*, nella quale è possibile selezionare la posizione in cui si desidera spostare i file selezionati.

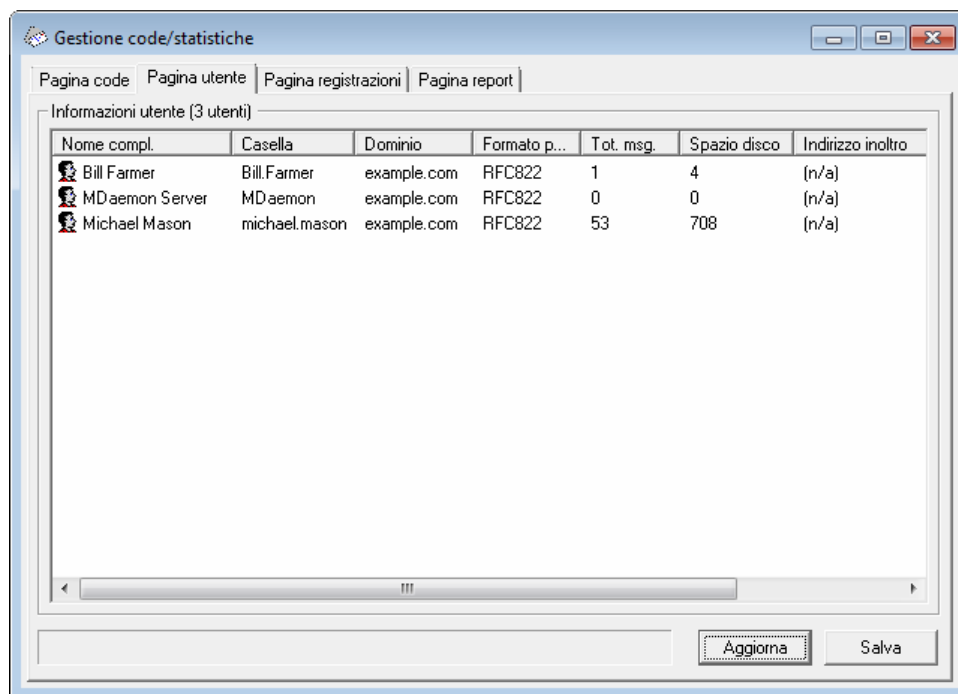
I file copiati o spostati in altre code di solito non conservano il nome originale. Per evitare di sovrascrivere gli eventuali file con lo stesso nome presenti nella coda, MDaemon calcola sempre il nome di file di destinazione in base al file `HIWATER.MRK` contenuto nella cartella di destinazione.

Elimina
Fare clic su questo pulsante per eliminare gli eventuali file selezionati nella casella di riepilogo relativa allo *stato della coda*. Verrà visualizzato un messaggio che indica di confermare l'eliminazione dei file selezionati.

Le code di posta vengono modificate dinamicamente mentre MDaemon è attivo grazie al trasferimento costante dei file di messaggio da e per le code. Per tale motivo, è necessario tenere presente che durante la copia, lo spostamento o l'eliminazione dei file può venire visualizzato un messaggio che

indica che l'operazione non può essere completata. Questa situazione si verifica quando il file di messaggio su cui si tenta di operare è già stato rimosso da MDaemon. Facendo clic sul pulsante *Aggiorna*, è possibile aggiornare l'elenco corrente dei file visualizzati nella casella di riepilogo.

Per impedire che durante le operazioni di modifica i messaggi vengano spostati all'esterno dalla coda, modificare le impostazioni del file `MDstats.ini`. A questo scopo, è sufficiente aprire il file `MDstats.ini` presente nella directory `\app\` di MDaemon e sostituire la chiave `LockOnEdit=No` in `[QueueOptions]` con `LockOnEdit=Yes`. In questo modo, ogni volta che si modifica un messaggio, viene creato un file `LCK` che impedisce che il messaggio soggetto a operazioni venga spostato all'esterno della coda.

10.3.2 Pagina utente

Informazioni utente

Quando si seleziona la *Pagina utente*, nella casella di riepilogo *Informazioni utente*viene caricato l'elenco di tutti gli account MDaemon. Nell'elenco sono specificati il nome completo dell'utente, il nome della casella postale, il dominio a cui appartiene l'account, il numero dei messaggi contenuti nell'account, il formato di posta, la quantità di spazio su disco (in KB) occupato dall'account, l'indirizzo di inoltro e la data relativa all'ultimo controllo della posta. Poiché l'elenco contiene informazioni in

costante cambiamento, è opportuno aggiornarlo facendo clic sul pulsante *Aggiorna*.

È possibile spostarsi all'interno della casella di riepilogo mediante le barre di scorrimento verticale e orizzontale oppure facendo clic in qualunque punto della casella di riepilogo e utilizzando i tasti FRECCIA. Le informazioni contenute nella casella di riepilogo *Informazioni utente* possono essere ordinate in base a qualunque colonna. È sufficiente fare clic una volta sulla colonna desiderata per ordinarla in modo ascendente (A-Z) oppure doppio clic per ordinarla in modo discendente (Z-A). Le colonne possono inoltre essere ridimensionate posizionando il puntatore sulla linea che separa le intestazioni di colonna finché non cambia forma, quindi trascinando la colonna fino a raggiungere la dimensione desiderata. Infine, è possibile fare doppio clic su qualunque voce per passare alla *Pagina code* e visualizzare il contenuto della casella postale corrispondente.

Per impostazione predefinita, nell'elenco viene visualizzato il conteggio dei messaggi (non dei file) e lo spazio utilizzato *dai messaggi* (non da tutti i file della directory). Queste sono le informazioni relative alle *Quote* riportate da MDaemon. In alternativa, è possibile visualizzare il conteggio dei *file* e lo spazio su disco utilizzato da tutti i *file* anziché dai messaggi. A questo scopo, è sufficiente aprire il file `MDstats.ini` presente nella directory `\app\` di MDaemon e sostituire la chiave `ShowQuota=Yes` di `[UserOptions]` in `ShowQuota=No`.

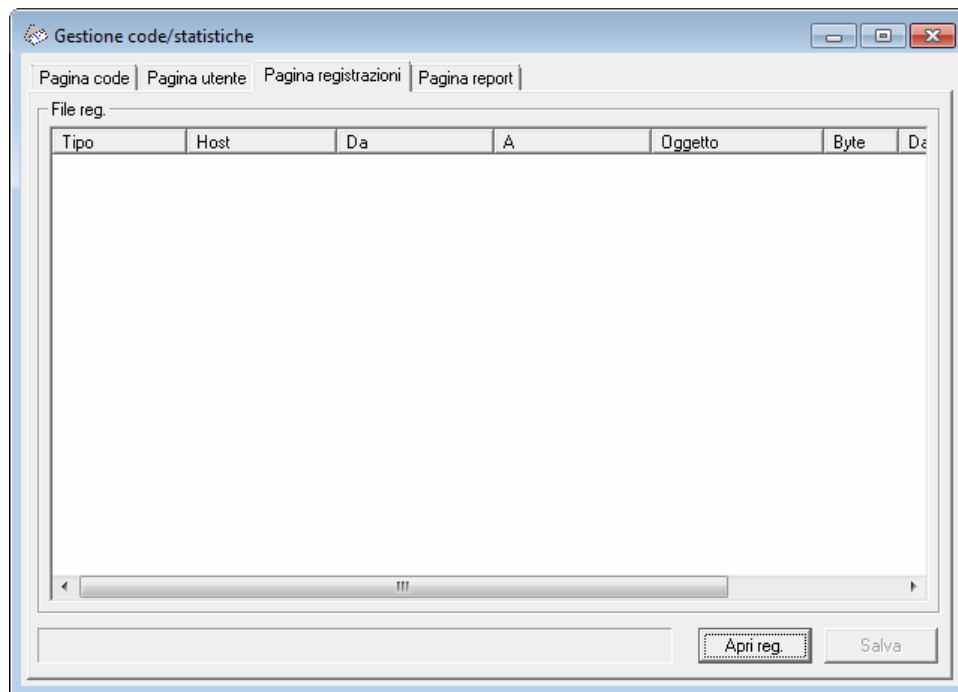
Le cartelle utenti contengono un file di nome "`hiwater.mrk`" che viene utilizzato per determinare alcune informazioni relative agli utenti. L'eventuale eliminazione di questo file impedirebbe a Gestione code e statistiche di ottenere alcune delle informazioni esposte nella casella di riepilogo *Informazioni utente*.

Aggiorna
Alcune statistiche relative agli utenti, ad esempio il numero di messaggi contenuti nella casella postale o la quantità di spazio su disco utilizzato dall'account, cambiano continuamente. È possibile aggiornare i contenuti della casella di riepilogo *Informazioni utente* semplicemente facendo clic sul pulsante *Aggiorna*. Verranno immediatamente visualizzate le informazioni correnti.

Indicatore di avanzamento
Poiché gli elenchi visualizzati nella casella di riepilogo *Informazioni utente* possono raggiungere dimensioni notevoli, al di sotto della casella di riepilogo è presente un indicatore di avanzamento che segnala visivamente che il programma è ancora in funzione mentre vengono caricati file di grandi dimensioni.

Salva
Facendo clic su questo pulsante, è possibile salvare i contenuti della casella di riepilogo *Informazioni utente* in formato delimitato da virgole, utilizzabile con i database, oppure come file di solo testo ASCII. Una volta scelti il nome e la

posizione da assegnare al file nella finestra Salva con nome di Windows, viene richiesto di specificare se salvare il file in formato delimitato da virgole o in formato di testo semplice.

10.3.3 Pagina registrazioni

Report registri

Nella casella di riepilogo *Report registri* vengono visualizzati i file di registro dettagliati di MDaemon, selezionabili mediante il pulsante *Apri registro* e la finestra di dialogo Apri di Windows. Il *Report dei registri* fornisce un metodo rapido e semplice per esaminare la cronologia delle transazioni di posta elaborate da MDaemon, senza che sia necessario controllare il notevole volume di informazioni che i file di registro di MDaemon talvolta contengono. Il report visualizzato nella casella di riepilogo è suddiviso in un formato semplice contenente: il tipo di messaggio (POP in entrata, DomainPOP, RFC822, e così via), l'host a cui si è connesso MDaemon durante la transazione, il mittente, il destinatario, le dimensioni del messaggio, la data di elaborazione di ciascun messaggio e l'esito della transazione.

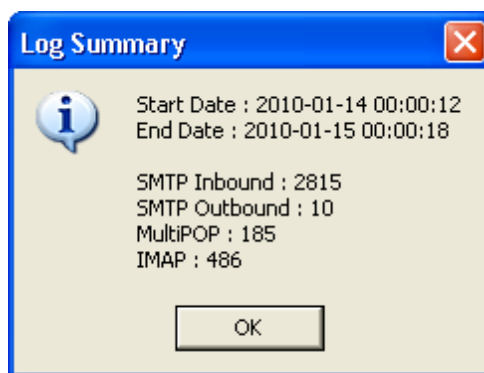
Per esaminare più dettagliatamente le voci del registro, è sufficiente fare doppio clic sulla voce desiderata. Verrà visualizzata la porzione di registro nella quale è stata eseguita la transazione. Mediante il menu di scelta rapida associato al clic con il pulsante destro del mouse, è possibile copiare e incollare la porzione dettagliata del registro in un editor di testo, quindi salvarla o modificarla.

È possibile spostarsi all'interno della casella di riepilogo mediante le barre di scorrimento verticale e orizzontale oppure facendo clic in qualunque punto della casella di riepilogo e utilizzando i tasti FRECCIA. Le colonne della casella di riepilogo possono inoltre essere ridimensionate posizionando il puntatore sulla linea che separa

le intestazioni di colonna finché non cambia forma, quindi trascinando la colonna fino a raggiungere la dimensione desiderata.

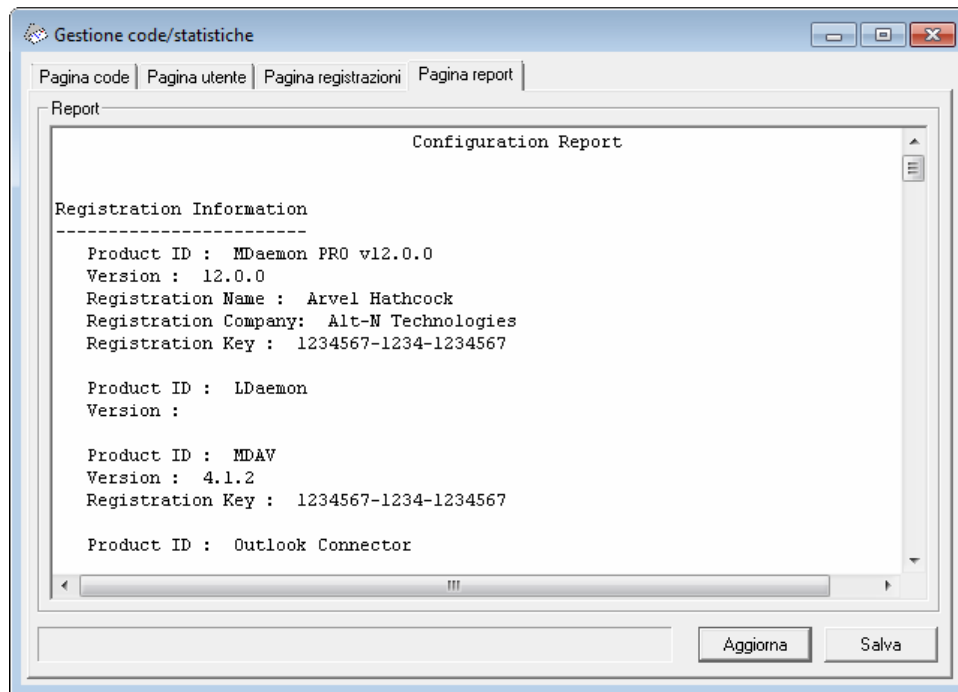
La scheda *Pagina registrazioni* consente di visualizzare i file registro creati mediante l'opzione *Registra sessioni posta dettagliate* o *Registra il riepilogo delle sessioni di posta* situate in Registrazione » Modalità di registrazione. Tuttavia, è consigliabile utilizzare l'opzione *Registra sessioni posta dettagliate*. Se si utilizza l'opzione *Registra il riepilogo delle sessioni di posta*, le informazioni visualizzate nel *Report registri* sono limitate. Dal momento che la *Pagina registrazioni* condensa il registro dettagliato in una visualizzazione di riepilogo dell'attività di MDaemon, fornendo comunque la possibilità di aprire una visualizzazione dettagliata di ogni transazione facendo doppio clic su una voce, non è necessario che MDaemon riepiloghi il file di registro in fase di compilazione.

Apri reg.
Fare clic su questo pulsante per aprire la finestra Apri di Windows e scegliere il file registro da visualizzare. Se si fa clic su questo pulsante quando un *file registro* è già visualizzato nella casella di riepilogo *Report registri*, è possibile aggiungere il nuovo file alla fine di quello visualizzato.

Una volta visualizzato un registro, viene aperta una finestra di messaggio contenente un riepilogo del registro selezionato. Quando si salva un report del registro come file di testo, a questo viene aggiunto il riepilogo del registro.

Indicatore di avanzamento
Poiché i *file registro* possono avere dimensioni notevoli, sotto la casella di riepilogo *Report registri* è presente un indicatore di avanzamento che segnala visivamente che il programma è ancora in funzione durante il caricamento o il salvataggio di file di grandi dimensioni.

Salva
Facendo clic su questo pulsante, è possibile salvare i contenuti della casella di riepilogo *Report registri* in formato delimitato da virgole, utilizzabile con i database, oppure come file di solo testo ASCII. Una volta scelti il nome e la posizione da assegnare al file nella finestra Salva con nome di Windows, viene richiesto di

specificare se salvare il file in formato delimitato da virgole o in formato di testo semplice.

10.3.4 Pagina report

Report
Facendo clic sulla *Pagina report*, viene prodotto un report esaustivo in cui sono elencate tutte le impostazioni di MDaemon in un formato di testo di facile lettura. Questa funzione consente all'amministratore di velocizzare le operazioni di controllo delle numerose impostazioni di configurazione di MDaemon e facilita la risoluzione dei problemi eventualmente riscontrati.

È possibile spostarsi nel report mediante le barre di scorrimento o i tasti CURSORE. Inoltre, fungendo anche da editor di testo, la visualizzazione del *Report* consente di inserire annotazioni o informazioni supplementari prima che se ne esegua il salvataggio in un file. È anche possibile utilizzare il menu di scelta rapida per tagliare, copiare e incollare in/da questa visualizzazione. A questo scopo, fare clic con il pulsante destro del mouse, quindi selezionare l'opzione desiderata dal menu visualizzato.

Aggiorna
Fare clic su questo pulsante per aggiornare il *report* delle impostazioni di MDaemon correntemente visualizzato.

Indicatore di avanzamento
Analogamente alle altre schede di Gestione code e statistiche, la *Pagina report* contiene un indicatore di avanzamento che offre una rappresentazione visiva del

funzionamento del programma mentre vengono caricati o salvati file di grandi dimensioni.

Salva
Fare clic su questo pulsante per salvare il *report* visualizzato. A seguito del clic su questo pulsante, verrà visualizzata una finestra di dialogo Salva con nome, in cui è possibile specificare il nome del file e la posizione in cui salvarlo.

10.3.5 Personalizzazione di Gestione code e statistiche

10.3.5.1 File MDstats.ini

Personalizzazione della funzione di gestione delle code e delle statistiche

Di seguito è riportato un elenco delle impostazioni modificabili dal file `MDstats.ini` presente nella directory `\app\` di MDaemon.

[MDaemon]

AppDir=C:\mdaemon\app\	Percorso della directory \app\ di MDaemon.

[QueueOptions]

Editor=NOTEPAD.EXE	Editor da utilizzare quando si fa doppio clic su un messaggio oppure si seleziona l'opzione Modifica dal menu visualizzato facendo clic con il pulsante destro del mouse.
LockOnEdit=No	Specifica se deve essere creato un file LCK quando si modifica un messaggio. Grazie a questa opzione, è possibile impedire che un messaggio in fase di modifica possa essere rimosso dalla coda.
AutoRefresh=Yes	Intervallo di tempo (in secondi) che deve trascorrere tra un aggiornamento automatico dell'elenco dei messaggi e un altro. Il valore 0 disattiva l'aggiornamento automatico.
ShowDirectories=Yes	Mostra le sottodirectory delle code presenti nella casella di riepilogo, oltre ai messaggi. Le directory vengono visualizzate nel formato <NomeDirectory>.

[UserOptions]

ShowQuota=Yes	Determina se nell'elenco degli utenti debbano essere visualizzate le informazioni sulle quote (calcolo dei messaggi e dello spazio su disco effettuato da MDaemon) o le informazioni sui file

	(numero di file e spazio su disco totale).
[LogOptions]	
ShowUnknown=Yes	Mostra le sessioni di' cui MDStats non è riuscito a determinare il tipo (in entrata o in uscita, SMTP o POP).
ShowSmtpInbound=Yes	Mostra le sessioni SMTP in entrata.
ShowPopInbound=Yes	Mostra le sessioni POP in entrata (controlli della posta).
ShowSmtpOutbound=Yes	Mostra le sessioni SMTP in uscita.
ShowPopOutbound=Yes	Mostra le sessioni POP in uscita (MultiPOP, DomainPOP).
ShowRFC822=Yes	Mostra le consegne di posta locale RFC822.
ShowSmtpHelo=Yes	Mostra il dominio HELO nella colonna Host per le sessioni SMTP in entrata.
IgnoreEmptyPop=Yes	Ignora i controlli della posta se non è stato consegnato alcun messaggio.
ShowImap=Yes	Mostra le sessioni IMAP.
[Remap]	Rimappatura delle lettere delle unità, utile per eseguire MDStats da un sistema diverso da quello su cui MDaemon è attivo.
C:=\\server\c	Durante la lettura di MDaemon.ini, sostituisce "C:" con "\\server\c".
[Special]	
OnlyOneInstance=No	Consente l'esecuzione di una sola istanza di MDStats. Se si tenta di riaprire MdStats, viene attivata l'istanza già in esecuzione.

Per ulteriori informazioni, vedere:

Parametri della riga di comando di MDStats 503

10.3.5.2 Parametri della riga di comando di MDStats

Nota: Nessun parametro della riga di comando è soggetto alla distinzione tra maiuscole e minuscole.

Numeri da 1 a 8	Consentono di visualizzare una coda specifica nella scheda Pagina code. = Coda remota = Coda locale = Coda tentativi = Coda LAN = Coda RAW = Coda messaggi scartati = Coda SmtpIn = Coda salvataggi
/L[N] [FileInput] [FileOutput]	Crea un report del file registro. Se si specifica la lettera "N" dopo "L", il report non viene salvato in formato delimitato da virgole.
/A	Creando un report del file registro, aggiunge le nuove informazioni al file di output anziché sovrascriverlo.

Sezione XI

11 Caratteristiche aggiuntive di MDaemon

11.1 MDaemon e file di testo

MDaemon utilizza numerosi file di testo al fine di memorizzare i propri dati, i modelli di messaggi generati dal sistema e le impostazioni di configurazione. Questa caratteristica offre un'ampia flessibilità. Per creare nuovi file di testo da MDaemon, selezionare File » Nuovo. Questa funzionalità può rivelarsi particolarmente utile per creare rapidamente dei file di dati da utilizzare con le risposte automatiche e con varie altre funzioni di MDaemon, ad esempio i file RAW.

Modifica dei file di MDaemon

I vari file di dati di MDaemon sono di testo semplice e si possono modificare con Blocco note. È possibile aprire direttamente i file con MDaemon mediante la selezione di menu File » Apri » File testo vuoto. Per impostazione predefinita, con questa selezione vengono cercati nella cartella `\app\` di MDaemon i file con estensione `*.txt`. Per visualizzare gli altri file della cartella, nell'elenco a discesa *Tipo file:* selezionare "Tutti i file".

11.2 Controllo remoto del server via e-mail

Utilizzando il sistema di trasporto e-mail, è possibile accedere a molte funzioni di MDaemon in modalità remota. Gli utenti possono ad esempio accedere a diversi aspetti dei propri account e modificarli o riconfigurarli inviando messaggi e-mail al server. MDaemon mantiene un account per l'utilizzo interno nel database utenti. L'account è accessibile inviando un messaggio alla casella postale "`MDaemon@MDaemonsDomain.com`". I messaggi inviati al server vengono memorizzati nella directory messaggi del server, analogamente a quanto avviene per gli utenti normali. All'esecuzione della coda, il server passa in rassegna tutta la posta ricevuta e analizza la sintassi di ciascun messaggio per rilevare la presenza di istruzioni speciali.

Alcuni di questi messaggi di controllo richiedono un account valido sul server e sono protetti da password. Per i comandi che richiedono un account valido, è necessario che il messaggio venga autenticato durante l'elaborazione SMTP mediante SMTP AUTH.

I comandi che possono essere utilizzati nei messaggi rientrano in tre categorie: Accesso e controllo dell'account 507, Controllo delle liste di distribuzione e dei cataloghi 508 e Comandi e-mail generali 511.

Vedere:

Accesso e controllo dell'account 507
Controllo dei cataloghi e delle liste di distribuzione 508
Comandi e-mail generali 511

11.2.1 Accesso e controllo degli account

Nella sezione seguente viene fornito l'elenco dei comandi per l'accesso e il controllo degli account disponibili per i titolari degli account. Per tutti questi comandi è necessario che il messaggio sia autenticato mediante SMTP AUTH. I parametri contenuti tra parentesi sono facoltativi. Ad esempio, "`nome [indirizzo]`" può essere immesso semplicemente come "`Luisa`" oppure con l'aggiunta di un parametro opzionale: "`Luisa LLiguori@dailyplanet.com`". Per ulteriori informazioni sull'uso di questo tipo di comandi nei messaggi e-mail, vedere: Controllo remoto del server via e-mail 506.

COMANDO	PARAMETRI	DESCRIZIONE
`ACCOUNT INFO`	nessuno	Lo stato dell'account passato nella riga dell'oggetto viene reinviato all'originatore. Esempio: `ACCOUNT INFO`
`PASSWORD`	nuova password	La password dell'account passata nella riga dell'oggetto viene trasformata in quella specificata. Esempio: `PASSWORD kryptonite`
`BEGIN SIGNATURE`	nessuno	Avvia la registrazione di un nuovo file di firma da allegare ai messaggi generati dall'account passato nella riga dell'oggetto. Le righe successive vengono considerate come testo del file di firma finché non viene rilevata la parola END in una riga a sé stante o non viene raggiunta la fine del messaggio di controllo. NOTA: la funzione per la firma è disponibile solo per i messaggi in formato RAW. Alla posta RFC-2822 in arrivo al server che utilizza SMTP o POP non viene aggiunto il file di firma. In questi casi, consultare la documentazione del client di posta in uso per informazioni sui file di firma.

`BEGIN AUTORESPONDER`	nessuno	Avvia la registrazione di un nuovo file di risposta automatica. Le righe successive vengono considerate come testo della risposta automatica finché non viene rilevata la parola END in una riga a sé stante o non viene raggiunta la fine del messaggio di controllo.
		
		Esempio:
		
		`BEGIN AUTORESPONDER`
		
		`Sono in vacanza. Tornerò presto.`
		
		`END`
		
		Per cancellare una risposta automatica attiva, utilizzare lo stesso comando senza specificare alcun testo di risposta.

		Esempio:
		`BEGIN AUTORESPONDER`
		`END`

`FORWARD TO`	indirizzo	L'indirizzo di inoltro per l'account passato nella riga dell'oggetto viene trasformato in [indirizzo] e per l'account viene attivato l'inoltro della posta. Es: `FORWARD TO vacanza@host.com`
`UNFORWARD`	nessuno	L'inoltro della posta viene disattivato per l'account specificato nella riga dell'oggetto. Es: `UNFORWARD`
`MULTIPOP`	on/off	MultiPOP viene attivato o disattivato per l'account specificato nella riga dell'oggetto. Es: `MULTIPOP ON` Es: `MULTIPOP OFF`

Per ulteriori informazioni, vedere:

Controllo remoto del server via e-mail 506
Controllo dei cataloghi e delle liste di distribuzione 508
Comandi e-mail generali 511

11.2.2 Controllo dei cataloghi e delle liste di distribuzione

Poiché nessuno di questi comandi richiede un account sul server, non è necessario che la riga dell'oggetto contenga dei valori speciali quando si specificano queste istruzioni. I parametri racchiusi tra [parentesi quadre] sono opzionali. Ad esempio, "`nome [indirizzo]`" può essere immesso semplicemente come "`Carlo`" oppure con l'aggiunta di un parametro opzionale: "`Carlo CRossi@dailyplanet.com`". Per ulteriori informazioni sull'uso di questo tipo di comandi nei messaggi e-mail, vedere: Controllo remoto del server via e-mail 506.

COMANDO	PARAMETRI	DESCRIZIONE
`SUBSCRIBE`	nomelista [indirizzo] [{nome reale}] [(password)]	L'originatore viene aggiunto alla lista specificata, purché la lista esista e consenta le iscrizioni remote. Se viene specificato un indirizzo opzionale dopo il nome della lista, alla lista viene aggiunto tale indirizzo anziché l'indirizzo trovato nel campo FROM: del messaggio di iscrizione. È possibile aggiungere il nome reale dell'iscritto racchiudendolo tra parentesi graffe, ad esempio {Franco Tommaso}. Se dopo il comando viene

		specificata la password della lista (le parentesi sono obbligatorie), il comando viene soddisfatto anche se la funzione per l'iscrizione della lista è disattivata.
		Esempi:
		`SUBSCRIBE mdsupp`
		`SUBSCRIBE mdsupp io@miodominio.com {Franco T}`
		`SUBSCRIBE mdsupp tu@tuodominio.com (PASS)`

`UNSUBSCRIBE` o `SIGNOFF`	nomelista [indirizzo] [(password)]	L'originatore viene rimosso dalla lista specificata, purché la lista esista e contenga l'originatore tra i suoi iscritti. Se viene specificato un indirizzo opzionale dopo il nome della lista, dalla lista viene rimosso tale indirizzo anziché l'indirizzo rilevato nel campo FROM: del messaggio di annullamento dell'iscrizione. Se dopo il comando viene specificata la password della lista (le parentesi sono obbligatorie), il comando viene soddisfatto anche se la funzione per il ritiro dalla lista è disattivata.
		Esempi:
		`UNSUBSCRIBE MDSUPP (MDSPASS)`
		`SIGNOFF MDSupportList io@miodominio.com`

`DIGEST`	nomelista [indirizzo]	Consente di impostare la ricezione della posta della lista in formato riassunto per il mittente. Se viene specificato un indirizzo opzionale dopo il nome della lista, la modalità riassunto viene impostata per tale indirizzo.
		Esempi:
		`SET DIGEST MDSupportList`
		`SET DIGEST mdsupp gianni@mdaemon.com`

`NORMAL`	nomelista [indirizzo]	Il mittente viene impostato per ricevere la posta dalla lista in formato normale (non riassunto). Se viene specificato un indirizzo opzionale dopo il nome della lista, la ricezione della posta in formato normale viene impostata per tale indirizzo e non per il mittente originale.
		Esempi:
		`NORMAL MDSupportList@miodominio.com`
		`NORMAL mdsupp@dominio.com gianni@altn.cc`

NOMAIL	nomelista [indirizzo]	Questo comando imposta la modalità nomail (no posta) per l'indirizzo. L'account viene posto in stato di sospensione e non riceve più il traffico della lista. Se non viene specificato alcun indirizzo, viene utilizzato l'originatore del messaggio. Esempio: `NOMAIL lista@nomedominio.com io@nomedomi`

MAIL	nomelista [indirizzo]	Questo comando reimposta la modalità normale (consegna della posta) per l'indirizzo precedentemente in modalità nomail. Se non viene specificato alcun indirizzo, viene utilizzato l'originatore del messaggio.
		Esempi:
		`MAIL lista@nomedominio.com`
		`MAIL lista@nomedominio.com io@nomedomini`

REALNAME	nomelista [indirizzo] {nome reale}	Questo comando imposta sul valore specificato il nome reale di "indirizzo", iscritto alla lista "nomelista". Il nome reale deve essere racchiuso tra i caratteri "{" e "}". Esempio: `REALNAME AssistMD@altn.com {Franco Tomma`
GET	nome-magico catalogo (password)	Recupera dal catalogo specificato un file, che viene codificato da MIME in un messaggio e-mail, e invia quest'ultimo all'account di origine o a quello specificato in una direttiva RESULTS TO. Esempio: `GET fileutili questofile (password)` **NOTA**: lo speciale catalogo PUBLIC non richiede un nome di catalogo o una password per il recupero di un file.
DIR	catalogo	Recupera una directory dei file e dei nomi magici disponibili nel catalogo. Esempio: `DIR public`
LIST	[nome lista] [password lista]	Offre informazioni sulla lista di distribuzione. Se il nome della lista non viene indicato, viene restituito un

riepilogo di tutte le liste. Se per le liste si indica una password, vengono restituite maggiori informazioni.

Esempio:

`LIST Lista@esempio.com Lz$12`

Per ulteriori informazioni, vedere:

Controllo remoto del server via e-mail 506
Accesso e controllo degli account 507
Comandi e-mail generali 511

11.2.3 Comandi e-mail generali

I comandi e-mail generali possono essere inviati all'account di sistema mediante messaggi e-mail. Per ulteriori informazioni su questo tipo di comandi, vedere: Controllo remoto del server via e-mail 506.

COMANDO	PARAMETRI	DESCRIZIONE
`HELP`	nessuno	Una copia di NEWUSERHELP.DAT viene elaborata e reinviata all'originatore del messaggio.

`RESULTS TO`	indirizzo	I risultati delle istruzioni successive vengono reinviati all'indirizzo e-mail specificato anziché a quello dell'originatore del messaggio.
		Esempio:
		`RESULTS TO nome@luogo.com`
		`LIST MDSUPP`

`STATUS`	nessuno	Un report sullo stato delle operazioni del server e sulle condizioni correnti viene reinviato all'originatore del messaggio. Poiché le informazioni presenti in questo report sono considerate riservate, è necessario che l'utente che richiede il report venga autenticato come amministratore. Esempio: `STATUS`

Per ulteriori informazioni, vedere

[Controllo remoto del server via e-mail] 506
[Accesso e controllo dell'account] 507
[Controllo dei cataloghi e delle liste di distribuzione] 508

11.3 Specifica dei messaggi RAW

11.3.1 Specifica dei messaggi RAW

MDaemon incorpora il supporto per un formato di messaggi e-mail semplice e potente, noto come RAW. Il sistema di posta RAW fornisce un formato semplice e standard, utilizzabile dai sistemi software come MDaemon per creare messaggi compatibili con il più complesso metodo RFC-2822. L'utilizzo di un sistema MTA come RAW fa sì che il software client deleghi al server la responsabilità della conformità con gli standard della posta Internet.

La posta RAW consiste in una serie di intestazioni testuali necessarie e opzionali seguite da un corpo del messaggio. La maggior parte delle intestazioni è costituita da un token seguito da un valore compreso tra i simboli <>. Ciascuna riga dell'intestazione termina con una combinazione <CRLF> di caratteri. Le intestazioni sono separate dal corpo del messaggio da una riga bianca e non sono sensibili alla distinzione tra maiuscole e minuscole. Inoltre, le intestazioni *Da* e *A* sono le uniche necessarie. Tutti gli elementi di testo, sia dell'intestazione che del corpo, sono in testo ASCII semplice e devono essere contenuti in un file con estensione "`RAW`", ad esempio "`mio-messaggio.raw`". Quindi, per accodare il messaggio per la consegna, collocare il file con estensione `RAW` nella coda RAW di MDaemon che, in genere, si trova in "`C:\MDaemon\Queues\Raw`".

Come ignorare Filtro contenuti

Per impostazione predefinita, i messaggi RAW vengono trasferiti tramite il Filtro contenuti come messaggi normali. Se si desidera che il filtro ignori un determinato messaggio RAW, è necessario che il nome del file inizi con "`p`" o con "`P`". Ad esempio, "`P_mio-messaggio.raw`" verrà ignorato da Filtro contenuti che, al contrario, elaborerà normalmente "`mio-messaggio.raw`".

Ignorando il Filtro contenuti, non è possibile applicare ai messaggi una firma DK o DKIM. Se MDaemon è stato configurato per firmare tutti i messaggi, ciò potrebbe provocare alcuni problemi di consegna. Se si desidera che MDaemon firmi i messaggi RAW configurati per ignorare il Filtro contenuti, è possibile utilizzare l'opzione `x-flag=sign` descritta di seguito.

Intestazioni RAW

From <casellapostale@host.com>	Questo campo contiene l'indirizzo e-mail del mittente.
To <casellapostale@host.com [, casellapostale@host.com]>	Questo campo contiene gli indirizzi e-mail dei destinatari. È possibile specificare più destinatari separandoli con una virgola.
ReplyTo <casellapostale@host.com>	Un indirizzo e-mail opzionale a cui vengono dirette le risposte al messaggio.
CC <casellapostale@host.com [, casellapostale@host.com]>	Un elenco opzionale di destinatari in copia conoscenza del messaggio. È possibile specificare più destinatari separandoli con una virgola.
Subject <testo>	Un oggetto opzionale per il messaggio.
Header <intestazione: valore>	Consente di inserire esplicitamente delle combinazioni intestazione/valore nel messaggio. Ciò consente di sostituire intestazioni personalizzate o non standard nei messaggi RAW

Campi speciali previsti dalla specifica RAW

Allegati di file e codifica

`x-flag=attach <percorsofile, metodo> [-x]`

Esempio: `x-flag=attach <c:\utils\pkzip.exe, MIME> -x`

X-FLAG specifica il valore "ATTACH" insieme a due parametri compresi tra i caratteri <>. Il primo parametro è il percorso completo del file da allegare al messaggio. Il secondo parametro, separato dal primo mediante una virgola, specifica il metodo di codifica da utilizzare per allegare il messaggio. In MDaemon sono supportati due valori per questo parametro. Il metodo MIME segnala al server di utilizzare il metodo standard Internet Base64 di codifica dei messaggi. Il metodo ASCII segnala al server di importare semplicemente il file nel messaggio. Il parametro -X opzionale alla fine della stringa indica al server di rimuovere il file dal disco una volta allegato.

Notifica dello stato della consegna

`x-flag=confirm_delivery`

Quando si converte in RFC-2822 un messaggio RAW che contiene questo flag, la stringa viene trasformata nel costrutto "Return-Receipt-To:@ <mittente@host.org>".

Inserimento di specifiche combinazioni intestazione/valore nel messaggio RFC-2822

```
Header <intestazione: valore>
```

Per inserire una combinazione intestazione/valore specifica nel messaggio RFC-2822 generato da un file RAW, è necessario utilizzare la macro HEADER indicata nella sezione Intestazioni RAW. Se ad esempio si desidera che l'intestazione "Delivered-By: computer-posta@dominio.com" venga inserita nel messaggio RFC-2822, occorre inserire "header <Delivered-By: computer-posta@dominio.com>" nel messaggio RAW. Per la macro "header" sono necessari sia il campo che il valore. In un messaggio RAW è possibile inserire un numero illimitato di macro "header".

Messaggi RAW con firma DK/DKIM

```
x-flag=sign
```

L'inclusione di questo comando speciale in un file con estensione `RAW` consente di applicare una firma DK/DKIM al messaggio RAW. Questo comando può essere utilizzato solo nei messaggi RAW configurati per ignorare il Filtro contenuti, ossia quelli il cui nome file inizia con "`p`" o con "`P`". Non è necessario utilizzare questo comando nel caso di messaggi RAW normali, elaborati tramite il filtro, che verranno firmati normalmente.

In tutti i messaggi RAW generati da Filtro contenuti viene utilizzato automaticamente il comando `x-flag=sign`.

Esempi di messaggi di posta RAW

Esempio 1:

```
from <mdaemon@altn.com>
to <JohnSmith@luogo.com>

Ciao John!
```

Esempio 2:

```
from <JohnSmith@luogo.com>
to <Presidente@CasaBianca.gov>
subject <File FBI segreti>
X-FLAG=CONFIRM_DELIVERY
X-FLAG=ATTACH <c:\secret\files\dole.zip, MIME> -X

Ecco tutti i file richiesti.
```

11.4 File semaforo

MDaemon offre il supporto per i file semaforo che possono essere utilizzati per diversi scopi, tra cui determinare specifiche azioni di MDaemon. MDaemon esegue una

scansione periodica della sottocartella `\APP\` per verificare l'esistenza di questi file. Se ne individua uno, viene attivato il comportamento appropriato e il file semaforo viene rimosso. Si tratta di un semplice meccanismo che consente agli amministratori e/o agli sviluppatori di gestire MDaemon senza utilizzarne l'interfaccia. Di seguito è riportato un elenco di tutti i file semaforo e delle azioni a essi associate:

NOME FILE	**AZIONE**
ADDUSER.SEM	Questo file semaforo consente di creare nuovi account. Viene utilizzato per imporre a MDaemon di aggiungere nuovi record alla fine del file USERLIST.DAT senza avviare una ricostruzione completa del database utenti, che potrebbe richiedere un periodo di tempo eccessivo. Ogni riga del file deve costituire un record di account completo nella forma specificata nella sezione Account Management Functions dell'API di MDaemon (vedere MD-API.html nella sottocartella \docs\API\ di MDaemon). È possibile specificare più account nuovi, un record di account per riga. MDaemon elabora il file una riga per volta e aggiunge un nuovo account. È possibile creare un file ADDUSER.LCK per bloccare il file in corso di aggiornamento in modo che MDaemon non intervenga su ADDUSER.SEM finché ADDUSER.LCK non sia stato eliminato. Per visualizzare un file ADDUSER.SEM di esempio, aprire ADDUSER.SMP nella directory APP con un editor di testo.
ALERT.SEM	Consente a tutti gli utenti WorldClient connessi al momento della creazione del file di visualizzare in una finestra popup il contenuto del file semaforo. Il contenuto del file non risulta immediatamente visibili a tutti gli utenti, ma viene reso disponibile a ciascun utente singolarmente quando questi inoltra una richiesta al server WorldClient tramite il proprio browser. **Nota:**diversamente dagli altri, questo è un file semaforo specifico di WorldClient e anziché nella directory \app\, deve essere inserito nella directory \MDaemon\WorldClient\.
ALIAS.SEM	Carica nuovamente i file di dati degli alias.
AUTORESPEXCEPT.SEM	Ricarica i file delle eccezioni della risposta automatica.
BATV.SEM	Carica nuovamente i file di dati della protezione

backscatter (BATV).

BAYESLEARN.SEM	Questo file semaforo avvia manualmente il processo di apprendimento bayesiano, così come avviene facendo clic sul pulsante Apprendi nella scheda Bayesiano di Spam Filter. Nota: con questa operazione, la procedura di apprendimento bayesiano viene avviata anche se l'apprendimento bayesiano è disattivato.
BESBACKUP.SEM	Questo file SEM consente di avviare un backup del database BES, analogamente a quanto avviene facendo clic sul pulsante *Backup dei file di database BES* in: BES BlackBerry » Backup/Ripristino 178.
BLACKLIST.SEM	Carica nuovamente i file di dati della lista nera.
CATLIST.SEM	Carica nuovamente la cache interna con i nomi dei cataloghi.
CFILTER.SEM	Ricarica le regole di Filtro contenuti, cancella i dati di Filtro contenuti presenti nella cache, ricarica il file Lista bianca (nessun filtro) 259 di Spam Filter.
CLEARQUOTACOUNTS.SEM	I risultati delle verifiche delle quote relative agli utenti vengono conservati nel file `quotacounts.dat`. Se si desidera cancellare il valore della quota relativa a un utente memorizzato nella cache, aggiungere l'indirizzo e-mail dell'utente nel file SEM e collocarlo nella cartella `\app\`. Se in una riga è presente solo un asterisco (*), l'intero file verrà eliminato invalidando tutti i conteggi delle quote memorizzate nella cache.
DELUSER.SEM	È possibile utilizzare questo file semaforo per eliminare uno o più account utente. Creare un file di testo contenente gli indirizzi di ciascun account che si desidera eliminare (un indirizzo per riga), denominare il file `DELUSER.SEM`, quindi spostarlo nella directory `\app\` di MDaemon. MDaemon eliminerà dapprima gli account, quindi il file `DELUSER.SEM`.
DOMAINSHARING.SEM	Carica nuovamente il file di dati di Condivisione dominio.
EDITUSER.SEM	Questo semaforo consente di aggiornare record

specifici del file USERLIST.DAT senza ricorrere a una ricostruzione completa, che potrebbe richiedere molto tempo. Per aggiornare un determinato record di USERLIST.DAT, è innanzitutto necessario costruire un record sostitutivo completo in base al formato specificato nella sezione Account Management Functions (Funzioni di gestione account) dell'API di MDaemon (vedere MD-API.html nella sottocartella \docs\API\ di MDaemon). Il nuovo record rispecchia le modifiche da aggiornare in USERLIST.DAT. I record di USERLIST.DAT da aggiornare vengono riconosciuti preponendo al nuovo record l'indirizzo e-mail del record originale, seguito da una virgola. Il file EDITUSER.SEM può contenere più record da aggiornare, ciascuno su una riga separata. MDaemon elabora il file una riga per volta. È possibile creare un file EDITUSER.LCK per bloccare il file in corso di aggiornamento in modo che MDaemon non intervenga su EDITUSER.SEM finché EDITUSER.LCK non sia stato eliminato. Per visualizzare un file EDITUSER.SEM di esempio, aprire EDITUSER.SMP nella directory \APP\ con un editor di testo.

EXCPTION.SEM	Impone a MDaemon di ricaricare il file EXCPTION.DAT.
EXITNOW.SEM	Chiude MDaemon.
GATEWAYS.SEM	Per offrire migliori prestazioni, MDaemon conserva nella memoria l'elenco dei gateway. Per ricaricare in MDaemon il file gateways.dat, creare il file GATEWAYS.SEM nella directory APP di MDaemon.
GREYLIST.SEM	Carica nuovamente i file di dati Greylisting.
GROUPS.SEM	Carica nuovamente i file di dati dei gruppi di account.
GRPLIST.SEM	Carica nuovamente la cache interna con i nomi delle liste di distribuzione.
HANGUPG.SEM	Impone un'interruzione condizionata del dispositivo RAS. MDaemon attende la chiusura delle eventuali sessioni di posta in sospeso, quindi interrompe la sessione RAS.
HANGUPR.SEM	Impone un'interruzione incondizionata del dispositivo

RAS. Si tratta di un'interruzione immediata e incondizionata, che prescinde delle sessioni di posta eventualmente in corso sulla connessione.

HOSTSCREEN.SEM	Carica nuovamente i file di dati di Vaglio host.
IPSCREEN.SEM	Carica nuovamente i file di dati di Vaglio IP.
LDAPCACHE.SEM	Carica nuovamente i file di dati degli utenti relativi a LDAP e gateway.
LOCKSEMS.SEM	Impedisce l'elaborazione di tutti i file semaforo fino alla sua rimozione.
LOGSETTINGS.SEM	Carica nuovamente le impostazioni del file di registro.
MDSPAMD.SEM	Carica nuovamente sia la lista bianca di Spam Filter sia MDSPAMD, con la conseguente reinizializzazione di tutti i relativi dati di configurazione.
MXCACHE.SEM	Carica nuovamente i file di dati della cache MX.
NODNSBL.SEM	Carica nuovamente il file della lista bianca DNSBL.
ONLINE.SEM	MDaemon crea questo file di semaforo quando stabilisce una connessione all'ISP mediante RAS e lo rimuove al termine della connessione. Il file si rivela utile per sapere se MD sta utilizzando il sottosistema RAS.
POSTDIAL.SEM	MDaemon crea questo file immediatamente dopo la chiusura della connessione effettuata in precedenza.
PREDIAL.SEM	MDaemon crea questo file immediatamente prima che si tenti di utilizzare il servizio di accesso remoto (RAS/DUN). in modo che gli altri programmi software liberino la porta di connessione quando questa deve essere utilizzata da MDaemon.
PRIORITY.SEM	Carica nuovamente i file di dati della posta prioritaria.
PROCBAD.SEM	Avvia la consegna del contenuto della coda dei

messaggi scartati.

`PROCDIG.SEM`	Avvia la creazione e la consegna dei riassunti della lista di distribuzione.
`PROCHOLDING.SEM`	Avvia la consegna del contenuto della coda trattenuta.
`PROCNOW.SEM`	Avvia il controllo della posta remota e la consegna di quella in coda. **Nota:** quando si invia un messaggio a "`procnow@nomedominio.com`" MDaemon genera il file `PROCNOW.SEM`. Di conseguenza, non è possibile utilizzare "`procnow`" come casella postale e-mail per un account.
`PROCREM.SEM`	MDaemon passa immediatamente in modalità di elaborazione della posta ed effettua le transazioni relative a tutta la posta remota.
`PROCRETR.SEM`	Avvia la consegna del contenuto della coda tentativi.
`PRUNE.SEM`	Carica nuovamente le impostazioni di sfoltimento automatico.
`QUEUERUN.SEM`	MDaemon crea questo file semaforo prima che inizi una sessione di posta. All'interno del file si trova un indicatore della data e dell'ora relative all'intervallo di elaborazione della posta più recente.
`RESTART.SEM`	Arresta e riavvia MDaemon.
`RESTARTCF.SEM`	Arresta e riavvia `CFEngine.exe`, ossia il file eseguibile di Filtro contenuti.
`RELOADCACHE.SEM`	Ricarica tutte le impostazioni e tutti i file memorizzati nella cache, ad eccezione delle impostazioni e dei file di Filtro contenuti.
`REVERSEEXCEPT.SEM`	Carica nuovamente il file delle eccezioni della ricerca inversa.
`SCHEDULE.SEM`	Carica nuovamente i file di dati della pianificazione.

SPAMHONEYPOTS.SEM	Carica nuovamente i file di dati delle trappole spam.
SPF.SEM	Carica nuovamente i file di dati relativi alle funzionalità SPF, DK, DKIM e VBR.
SUPPRESS.SEM	Carica nuovamente le impostazioni della lista nera e cancella quelle del dominio memorizzate nella cache.
TARPIT.SEM	Carica nuovamente i file di dati relativi a tarpit e a vaglio dinamico.
TRANSLAT.SEM	Ricarica il file di dati della traduzione delle intestazioni.
TRAY.SEM	Ridisegna l'icona di MDaemon nella barra delle applicazioni.
TRUST.SEM	Per offrire migliori prestazioni, i domini accreditati e gli indirizzi IP vengono conservati nella memoria residente. Per ricaricare manualmente tali impostazioni, creare TRUST.SEM.
UPDATEAV.SEM	Avvia l'aggiornamento delle definizioni virus di SecurityPlus per MDaemon.
UPDATESA.SEM	Avvia l'aggiornamento di Spam Filter.
USERLIST.SEM	Carica nuovamente il file USERLIST.DAT. Utilizzare questo file quando si effettuano delle modifiche a USERLIST.DAT ed è necessario che MDaemon lo ricarichi.
WATCHDOG.SEM	MDaemon cerca e rimuove questo semaforo dalla directory APP ogni 10-20 secondi circa. Questo file può essere utilizzato dalle applicazioni esterne per verificare se MDaemon è in esecuzione. Se questo file rimane nella directory APP per più di 20 secondi, è probabile che MDaemon non sia più in esecuzione.

11.5 Sistema di precedenza dei messaggi

Questa funzione consente di assegnare ai messaggi un valore di "precedenza", ovvero

un livello di importanza, compreso tra 0 e 99. Il valore indica l'ordinamento relativo dei messaggi durante il processo di consegna. Il valore è inversamente proporzionale all'importanza del messaggio e alla relativa posizione nell'ordine della coda dei messaggi. In altri termini, MDaemon tenta di consegnare un messaggio con valore 10 prima di un messaggio con valore 90. Di seguito sono riportate alcune indicazioni generali per l'assegnazione dei valori di precedenza: 10 = Urgente, 50 = Normale, 80 = Collettivo.

Le opzioni relative a questa funzionalità sono disponibili nella schermata Intestazioni200 di Preferenze e nella schermata Opzioni429 dell'editor delle liste di distribuzione. È inoltre possibile utilizzare l'azione di Filtro contenuti "*Add extra header item to message (Aggiungi intestazione al messaggio)*214" per inserire l'intestazione Precedence nei messaggi.

11.6 Route Slip

Di solito, all'interno di un file di messaggio in attesa in una coda sono contenute tutte le informazioni necessarie perché il messaggio venga consegnato alla destinazione appropriata. All'interno del file, inoltre, sono memorizzate le intestazioni, ad esempio X-MDaemon-Deliver-To, che forniscono a MDaemon le istruzioni sulla destinazione e sul destinatario del messaggio. In alcuni casi può tuttavia essere necessario o opportuno ignorare queste informazioni e fornire delle alternative specifiche sulla destinazione e sul destinatario di un messaggio. Il route slip fornisce esattamente questo meccanismo. Un route slip è un file che fornisce a MDaemon delle informazioni molto specifiche sulla destinazione e sul destinatario di un messaggio. Se per un particolare messaggio è presente un route slip, la destinazione e il destinatario del messaggio verranno controllati in base alle impostazioni del route slip e non a quelle del file .MSG stesso.

I route slip hanno estensione `RTE`. Ad esempio, se un file di messaggio in attesa di invio è denominato "`MD0000.MSG`", il route slip corrispondente avrà il nome `MD0000.RTE` e dovrà trovarsi nella stessa directory (coda di posta) del file di messaggio.

Un route slip presenta il seguente formato:

```
[RemoteHost]
DeliverTo=dominio-remoto.com
```

Questa sezione di un route slip indica a MDaemon il server a cui deve essere inviato il file `.MSG` corrispondente. MDaemon tenta sempre di stabilire una connessione diretta all'host cercando di instradare il messaggio nel più breve tempo possibile. È possibile specificare un solo host.

```
[Port]
Port=xxx
```

Questo comando specifica la porta utilizzata per i tentativi di connessione TCP/IP e di consegna. La porta predefinita per la posta SMTP è la porta 25.

```
[LocalRcpts]
Rcpt0=indirizzo@nome-dominio.com
Rcpt1=secondo-indirizzo@nome-dominio.com
Rcpt1=terzo-indirizzo@nome-dominio.com
```

```
[RemoteRcpts]
Rcpt0=indirizzo@dominio-esterno.com
Rcpt1=secondo-indirizzo@dominio-esterno.com
Rcpt1=terzo-indirizzo@dominio-esterno.com
```

Queste sezioni del route slip consentono di specificare il numero desiderato di destinatari locali e remoti per la ricezione di una copia del file `.MSG` associato. Gli indirizzi dei destinatari locali e remoti devono essere tenuti separati all'interno delle rispettive sezioni `[LocalRcpts]` e `[RemoteRcpts]`.

Benché forniscano un efficace meccanismo di consegna o reindirizzamento della posta elettronica, generalmente i route slip non sono necessari. MDaemon, ad esempio, utilizza i route slip per i messaggi di una lista di distribuzione "instradata". Quando una lista di distribuzione viene impostata per instradare una sola copia del messaggio di lista a un host remoto, viene utilizzato un route slip. Si tratta di un metodo molto efficace per consegnare la posta in caso di indirizzi collettivi. Per una singola copia del messaggio può infatti essere specificato un numero illimitato di destinatari. Tuttavia, non tutti gli host remoti consentono questo tipo di instradamento. Poiché in ultima istanza rappresentano i sistemi incaricati di consegnare una copia del messaggio a ciascun indirizzo, alcuni host pongono un limite sul numero di destinatari specificabili.

11.7 MDaemon e i server proxy

MDaemon è stato progettato appositamente per offrire un alto livello di versatilità. Di conseguenza, può essere configurato per funzionare in un'ampia gamma di tipi di rete e con una vasta scelta di prodotti. L'elevata flessibilità lo rende inoltre particolarmente adatto per operare con i server proxy LAN. Per configurare MDaemon per l'utilizzo di un server proxy, è sufficiente accertarsi che le impostazioni della porta in uso (vedere la sezione Porte49) non siano in conflitto con quelle eventualmente impostate nel server proxy. Ad esempio, la posta SMTP viene solitamente trasferita mediante la porta 25. Poiché un indirizzo IP può disporre di una sola porta 25, due server non possono ricevere contemporaneamente la posta SMTP sullo stesso sistema. Quando si tenta di integrare MDaemon con un proxy, è opportuno che il controllo sull'elaborazione e sulla consegna della posta venga svolto principalmente da MDaemon. Per conseguire questo scopo, può essere necessario disabilitare SMTP, POP, IMAP e diverse altre porte nel server proxy, così da consentire a MDaemon di gestire le operazioni di consegna della posta autonomamente.

Tuttavia, nel caso sia necessario incanalare la posta attraverso un proxy, MDaemon consentirà di configurare le porte da utilizzare per l'invio e la ricezione delle transazioni SMTP/POP/IMAP. Per filtrare le transazioni SMTP/POP/IMAP attraverso un server proxy o un firewall, potrebbe essere necessario impostare le porte su valori non standard.

Per informazioni più dettagliate su come configurare MDaemon per l'utilizzo con un server proxy, consultare le risorse disponibili nel sito www.altn.com.

Sezione XII

12 Glossario

ACL - Acronimo di **A**ccess **C**ontrol **L**ists. È un'estensione del protocollo Internet Message Access Protocol (IMAP4) che consente di creare un elenco di accesso per ogni cartella di messaggi IMAP disponibile, accordando diritti di accesso a tali cartelle anche agli altri utenti che dispongono di un account sullo stesso server di posta. Le autorizzazioni possono essere impostate in modo da limitare o estendere il livello di controllo che ciascun utente può esercitare su tali cartelle. È ad esempio possibile specificare se un utente è autorizzato a eliminare dei messaggi, a contrassegnarli come letti o non letti, a copiare i messaggi nelle cartelle, a creare delle nuove sottocartelle e così via. Solo i client e-mail che supportano ACL possono essere utilizzati per condividere l'accesso e impostare le autorizzazioni. Se il client e-mail in uso non supporta ACL, sarà comunque possibile impostare queste autorizzazioni dall'interfaccia di MDaemon.

Il protocollo ACL viene descritto approfonditamente nella RFC 2086, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2086.txt

ASCII - Acronimo di "**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange". Si tratta del codice standard utilizzato a livello mondiale per rappresentare tutte le lettere (maiuscole e minuscole) dell'alfabeto latino, nonché i numeri e i segni di interpunzione sotto forma di numeri binari a 7 cifre. A ogni carattere è assegnato un numero compreso tra 0 e 127 (da 0000000 a 1111111). Ad esempio, il codice ASCII per la lettera M maiuscola è 77. La maggior parte dei computer utilizza i codici ASCII per rappresentare il testo, in modo da poter trasferire i dati ad altri sistemi. La maggior parte degli editor e degli elaboratori di testo è in grado di memorizzare i file in formato ASCII (definiti, talvolta, semplicemente file ASCII). Tuttavia, la maggior parte dei file di dati, in particolare quelli che contengono dati numerici, non viene memorizzata in formato ASCII.

Diversi set di caratteri utilizzano 8 bit anziché 7 e dispongono quindi di 128 caratteri supplementari. Questi caratteri aggiuntivi sono utilizzati per rappresentare i simboli e i caratteri non appartenenti all'alfabeto inglese. Il sistema operativo DOS utilizza un set ASCII superiore, denominato ASCII esteso o "high ASCII". Uno standard riconosciuto a livello quasi universale è ISO Latin 1, utilizzato da numerosi sistemi operativi e browser Web.

ATRN - Vedere ETRN e ODMR più avanti.

Allegato - Un file allegato a un messaggio e-mail. Poiché la maggior parte dei sistemi di gestione e-mail supporta solo l'invio di file di testo, se l'allegato è costituito da un file binario o da un file di testo formattato (ad esempio, un documento creato con un elaboratore di testo), deve essere codificato come testo prima dell'invio e decodificato dopo la ricezione. Esistono numerosi schemi di codifica: i più diffusi sono le codifiche MIME (Multipurpose Internet Mail Extensions) e Uuencode (Unix-to-Unix). Per i messaggi in arrivo, il server MDaemon di Alt-N può essere configurato sia in modo che il processo di decodifica venga eseguito dal client e-mail del destinatario, sia per decodificare automaticamente gli allegati e memorizzarli in una posizione specifica prima di consegnare il messaggio all'utente locale.

Dorsale - Una linea o una serie di connessioni che formano il percorso principale di una rete. Si tratta di un termine alquanto relativo, dal momento che a volte una linea non di dorsale di una grande rete può avere dimensioni superiori alla dorsale di una rete più piccola.

Larghezza di banda - Quantità di dati che è possibile trasmettere in un intervallo prefissato di tempo mediante una connessione di rete o via modem, misurata generalmente in bit al secondo (o bps, bits-per-second). Una pagina intera di testo equivale a circa 16.000 bit, trasferibili da un modem veloce in circa 1 o 2 secondi. Un video a pieno schermo richiede quasi 10.000.000 bps, a seconda della compressione utilizzata.

La larghezza di banda può essere equiparata a un'autostrada. L'autostrada rappresenta la connessione, mentre i veicoli che la percorrono rappresentano i dati. Più larga è l'autostrada (quindi, maggiore è la larghezza di banda), maggiore è il numero di veicoli che possono percorrerla.

Baud - La velocità in baud rappresenta una misura della frequenza con cui i segnali portanti cambiano valore su una linea telefonica. Si riferisce alla velocità a cui un modem trasmette i dati. Solitamente, i modem più lenti vengono descritti in termini di velocità in baud, mentre quelli più veloci vengono classificati mediante bit al secondo. I due termini non sono necessariamente sinonimi, poiché ciascun segnale è in grado di codificare più di un bit nelle connessioni ad alta velocità.

Bit - Abbreviazione di **B**inary dig**it**. ovvero dell'unità di dato minima: un numero a cifra singola a base 2 (0 o 1). Il bit viene solitamente abbreviato con una "b" minuscola, come accade in "bps" (bits per second). Una pagina intera di testo corrisponde a circa 16.000 bit.

Bitmap - La maggior parte delle immagini visualizzate su un computer, comprese quelle presenti in Internet, è costituita da bitmap. Una bitmap è sostanzialmente una mappa di punti (o bit) che ha l'aspetto di un'immagine, almeno finché non viene osservata troppo da vicino o non viene ingrandita in misura eccessiva. I tipi di file bitmap più comuni sono BMP, JPEG, GIF, PICT, PCX e TIFF. Le immagini bitmap sono costituite da una serie di punti. Se vengono ingrandite, appaiono a blocchi e risultano poco uniformi. La grafica vettoriale, in genere creata nei formati CorelDraw, PostScript o CAD, consente invece un ingrandimento migliore, poiché è costituita da forme geometriche generate matematicamente anziché da punti disposti in modo apparentemente "casuale".

Bps - Acronimo di "**B**its **P**er **S**econd" (bit al secondo). È la misura della velocità con cui i dati possono essere trasferiti da una posizione all'altra. Ad esempio, un modem a 33,6 kbps è in grado di trasferire 33.600 bit al secondo. Kilobit (1000 bit) al secondo e Megabit (1.000.000 bit) al secondo vengono abbreviati rispettivamente in "Kbps" e "Mbps".

Browser - Abbreviazione di "Web browser". Si tratta di un'applicazione utilizzata per visualizzare le pagine Web. È in grado di interpretare codice HTML, testo, collegamenti ipertestuali, immagini, JavaScript e così via. I browser più diffusi sono Internet Explorer e Netscape Communicator.

Byte - Set di bit (di solito otto) che rappresenta un singolo carattere. Un byte contiene 8 o più bit, a seconda della modalità di misurazione. Il termine "byte" viene

abbreviato con una "b" maiuscola.

Cache - Esistono diversi tipi di cache, ma tutti vengono utilizzati per memorizzare i dati più recenti, così che a questi sia possibile accedere con maggiore rapidità in un secondo momento. Ad esempio, un browser Web utilizza una cache per memorizzare pagine, immagini, URL e altri elementi relativi a un sito Web visitato di recente. Quando si accede una seconda volta a una pagina memorizzata nella cache, il browser non deve scaricare di nuovo tali elementi. Poiché l'accesso alla cache sul disco fisso è molto più veloce dell'accesso a Internet, la consultazione delle pagine viene considerevolmente accelerata.

La cache degli IP di MDaemon memorizza gli indirizzi IP dei domini a cui sono stati recentemente inviati messaggi. In questo modo, MDaemon non deve cercare nuovamente tali indirizzi per consegnare eventuali altri messaggi agli stessi domini. Il processo di consegna diventa pertanto molto più rapido.

CGI - Acronimo di Common **G**ateway **I**nterface. Si tratta di un insieme di regole che descrivono il modo in cui un server Web comunica con altri programmi sullo stesso sistema e il modo in cui questi ultimi (i cosiddetti "programmi CGI") comunicano con il server Web. Un programma CGI è una qualunque applicazione che gestisce l'input e l'output in base allo standard CGI. Si tratta generalmente di un programma di piccole dimensioni che preleva i dati dal server Web e li elabora, ad esempio inserendo il contenuto di un modulo in un messaggio e-mail. I programmi CGI vengono spesso memorizzati nella directory "cgi-bin" di un sito Web e di solito sono visualizzati nell'URL utilizzato per accedervi.

cgi-bin - Il nome più comune per la directory di un server Web in cui sono memorizzati i programmi CGI. La porzione "bin" di "cgi-bin" è l'abbreviazione di "binary": precedentemente infatti numerosi programmi venivano considerati "binari". In realtà, la maggior parte dei programmi cgi-bin è costituita da file di testo, ovvero script eseguiti da programmi residenti altrove.

CIDR - Acronimo di "**C**lassless **I**nter-**D**omain **R**outing". Si tratta di un nuovo sistema di indirizzi IP che sostituisce il precedente, basato sulle classi A, B e C. Gli indirizzi IP CIDR hanno l'aspetto di normali indirizzi IP seguiti da una barra e da un numero, il cosiddetto prefisso IP. Ad esempio,

123.123.0.0/12

Il prefisso IP definisce il modo in cui molti indirizzi vengono coperti dall'indirizzo CIDR, con i numeri più bassi che coprono più indirizzi. Nell'esempio precedente il prefisso IP "/12" può essere utilizzato per indirizzare 4.096 indirizzi della precedente classe C.

Gli indirizzi CIDR riducono le dimensioni delle tabelle di instradamento e rendono più indirizzi IP disponibili all'interno delle organizzazioni.

Il sistema CIDR viene descritto nelle RFC 1517-1519, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Client - Programma utilizzato per accedere, nonché per ottenere e inviare dati da e a un programma *server*. Il server si trova di solito su un altro computer, che non deve necessariamente appartenere alla rete locale. Ciascun programma *client* è progettato per funzionare con uno o più tipi specifici di programmi *server*. Ciascun server richiede un tipo specifico di client. Un *browser* Web è un tipo specifico di client che comunica con i *server* Web.

Common Gateway Interface - Vedere CGI.

Cookie - Nella terminologia informatica, un *cookie* rappresenta una serie di dati inviati da un server Web al browser. Queste informazioni vengono salvate e successivamente utilizzate per diversi scopi, quando l'utente accede di nuovo allo stesso sito o ne visita una pagina diversa. Quando un server Web riceve da un browser Web una richiesta in cui è incluso un cookie, può utilizzare le informazioni del cookie per conseguire lo scopo per cui è stato progettato, ad esempio personalizzare i dati che invia all'utente o mantenere un registro delle richieste dell'utente. Di solito, i cookie vengono utilizzati per memorizzare password, nomi utente, preferenze, informazioni sui carrelli degli acquisti e altri dati associati al sito a cui i cookie corrispondono. In questo modo, il sito "riconosce" l'utente e riesce a tenere traccia delle relative attività.

A seconda delle impostazioni del browser, è possibile accettare o meno i cookie, nonché decidere per quanto tempo debbano essere conservati. I cookie sono in genere impostati per scadere dopo un determinato periodo e vengono preservati in memoria fino alla chiusura del browser, quando è possibile che vengano salvati sul disco.

I cookie **non** sono in grado di leggere dal disco rigido. Tuttavia, possono essere utilizzati per raccogliere informazioni sull'utente e le attività che questi esegue nel particolare sito a cui appartengono.

Connessione di accesso remoto - Componente di Windows che consente di connettere il computer alla rete mediante un modem. Se il computer non è connesso a una rete LAN con accesso a Internet, è necessario configurare l'accesso remoto (definito anche DUN, Dial-Up Networking) al fine di connettersi a un POP (Point of Presence) e accedere al provider di servizi Internet (o ISP, Internet Service Provider). Successivamente, sarà possibile ottenere l'accesso a Internet. Può essere necessario che il provider fornisca determinate informazioni, quali l'indirizzo del gateway e l'indirizzo IP del computer.

La connessione di accesso remoto è selezionabile facendo doppio clic sull'icona Risorse del computer. È possibile configurare un profilo di accesso differente per ciascun servizio online utilizzato. Una volta configurato, è possibile copiare sul desktop un collegamento al profilo. Per stabilire la connessione, sarà sufficiente doppio clic sull'icona del collegamento.

Predefinito - Termine utilizzato per fare riferimento al valore preimpostato per le opzioni dei programmi. Le impostazioni predefinite vengono utilizzate quando l'utente non specifica alcuna impostazione personalizzata. Ad esempio, l'impostazione predefinita per i caratteri in Netscape Communicator è "Times". L'impostazione rimarrà invariata finché non viene modificata dall'utente. La maggior parte degli utenti si avvale in genere delle impostazioni predefinite.

I valori predefiniti vengono frequentemente utilizzati se un'impostazione personalizzata non funziona oppure se al programma mancano alcuni dati per completare un'operazione.

DHCP - Acronimo di "**D**ynamic **H**ost **C**ontrol **P**rotocol". I server di rete utilizzano questo protocollo per assegnare dinamicamente gli indirizzi IP ai computer in rete. Un server DHCP attende che un computer stabilisca la connessione, quindi assegna al computer un indirizzo IP prelevandolo da un elenco presente in memoria.

Il sistema DHCP viene descritto nella RFC-2131, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2131.txt

Gateway di dominio - Vedere Gateway più avanti.

Nome dominio - Nome univoco che identifica un sito Web su Internet. Ad esempio, "altn.com" è il nome dominio di Alt-N Technologies. Ciascun nome dominio contiene due o più porzioni separate da punti: la porzione all'estrema sinistra è la più specifica mentre quella all'estrema destra è la più generica. Ciascun nome dominio punta all'indirizzo IP di un solo server, ma un server può avere più nomi dominio. Ad esempio, "mail.altn.com", "alt-n.com" e "dominio.com" possono puntare tutti allo stesso server di "altn.com", mentre "altn.com" non può puntare a due server diversi. Esistono tuttavia dei metodi per specificare dei server alternativi a cui i client vengono reindirizzati se il server principale è guasto o non disponibile.

Comunemente un nome di dominio viene registrato ma non effettivamente connesso a un sistema. Di solito, questo si verifica perché il proprietario del nome di dominio non ha ancora creato il sito Web oppure perché desidera disporre di indirizzi e-mail presso uno specifico dominio senza dover gestire un sito Web. In quest'ultimo caso, deve esistere un sistema Internet vero e proprio che gestisca la posta associata al nome dominio.

Infine, è frequente che il termine "nome dominio" venga abbreviato in "dominio". Tuttavia, poiché "dominio" ha altri significati e può fare riferimento ad altri elementi (ad esempio, un dominio di Windows NT o una classe di valori), è opportuno conoscere la distinzione al fine di evitare confusione.

I nomi dominio vengono descritti nelle RFC 1034-1035, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc1034.txt

http://www.rfc-editor.org/rfc/rfc1035.txt

DomainPOP - Sviluppato da Alt-N Technologies come componente del server MDaemon, DomainPOP consente di fornire servizi e-mail dalla casella postale POP di un singolo ISP per un'intera LAN o per un intero gruppo di lavoro. In precedenza, a meno che il server e-mail di un'azienda non disponesse di una connessione a Internet permanente, l'unico modo per fornire i servizi di posta Internet a un gruppo di lavoro consisteva nell'assegnare a ciascun utente una propria casella postale sull'ISP aziendale e raccogliere la posta da tale casella. Con DomainPOP è sufficiente una sola casella postale. L'ISP trasferisce tutta la posta per il nome dominio dell'azienda nella casella postale e da questa DomainPOP raccoglie periodicamente i messaggi. Quindi, analizza la sintassi dei messaggi per determinarne i destinatari e

distribuirli alle caselle postali degli utenti locali. In questo modo, il servizio e-mail viene fornito a un'intera rete da un singolo account ISP in accesso remoto.

Download (o scaricamento) - Processo mediante il quale il computer ottiene o recupera i dati da un altro computer. Le informazioni, ad esempio, vengono ottenute da Internet *scaricandole* da altri computer. L'operazione opposta allo scaricamento è il *caricamento*. Per inviare dati a un altro computer, è necessario *caricarli* nel computer in questione.

Driver - Programma di dimensioni ridotte che comunica con un determinato dispositivo hardware. I driver contengono le informazioni necessarie al computer e ad altri programmi per controllare e riconoscere il dispositivo. Nei computer Windows spesso i driver sono contenuti in un file DLL (Dynamic Link Library). La maggior parte dei dispositivi hardware utilizzati dai computer Mac non richiede driver. Tuttavia, nel caso fosse necessario, il driver presenterebbe la forma di un'estensione di sistema.

DUN - Vedere Connessione di accesso remoto.

E-mail - Abbreviazione di "Electronic mail" (posta elettronica). Il termine compare anche nelle forme "E-mail", "Email", "e-mail" ed "email". Si tratta della trasmissione di messaggi di testo mediante le reti di comunicazione. La maggior parte delle reti dispone di un sistema e-mail. Alcuni sono confinati su una rete composta da un solo computer, altri dispongono di gateway per accedere a reti diverse (comunicazione con più posizioni specifiche) o a Internet (comunicazione con qualunque luogo del mondo).

La maggior parte dei sistemi e-mail include sia un *client -mail* (definito anche *client di posta* o semplicemente *client*) contenente un editor di testo e altri strumenti per la composizione di messaggi, sia uno o più *server* che ricevono i messaggi dai client e li instradano alla destinazione appropriata. Di solito, un messaggio viene composto mediante il client, quindi trasferito al server per essere consegnato all'*indirizzo e-mail* specificato e infine instradato dal server a un altro server che si occupa della memorizzazione dei messaggi destinati a tale indirizzo. Se la destinazione del messaggio è un indirizzo locale di cui è responsabile il server originale, il messaggio può essere conservato su questo anziché essere instradato a un altro server. Infine, il destinatario del messaggio si connette al proprio server e ritira il messaggio mediante il proprio client e-mail. L'intero processo di trasferimento di un messaggio e-mail dal client al server di destinazione richiede solitamente pochi secondi o minuti.

Oltre al testo semplice, i messaggi e-mail possono contenere anche degli *allegati*, che possono essere file di qualsiasi tipo, ad esempio immagini, file di testo, programmi, altri messaggi e-mail e così via. Tuttavia, poiché la maggior parte dei sistemi e-mail supporta solo l'invio dei file di testo, gli allegati devono essere codificati (cioè, convertiti in formato di testo) prima di poter essere inviati, quindi decodificati quando raggiungono la destinazione finale. Questo processo viene di solito eseguito automaticamente dai client di posta di invio e di ricezione.

Tutti gli ISP offrono servizi e-mail. La maggior parte inoltre, supportando i gateway, consente di scambiare messaggi e-mail con altri sistemi di posta. Benché sistemi diversi possano elaborare la posta utilizzando protocolli diversi gli uni dagli altri, esistono tuttavia standard comuni che consentono di scambiare messaggi con gli utenti di praticamente qualunque sistema.

Indirizzo e-mail - Nome o stringa di caratteri che identifica una specifica casella postale elettronica presente su una rete a cui è possibile inviare dei messaggi e-mail. Gli indirizzi e-mail rappresentano le posizioni a cui e da cui vengono inviati i messaggi e-mail. Gli indirizzi e-mail sono necessari ai server e-mail per instradare i messaggi alle destinazioni appropriate. Benché a diversi tipi di rete corrispondano diversi formati di indirizzi e-mail, su Internet tutti gli indirizzi e-mail hanno la forma seguente: "casellapostale@dominio.com".

Ad esempio:

`Franco.Tommaso@altn.com`

Client e-mail - Definito anche *client di posta* (o semplicemente *client*), il *client e-mail* è un'applicazione che consente di inviare, ricevere e gestire la posta elettronica. Il nome client deriva dal fatto che i sistemi e-mail si basano su un'architettura client-server, in cui il client compone il messaggio e lo invia a un server e quest'ultimo instrada il messaggio al server del destinatario. Il messaggio viene infine ritirato dal client del destinatario. Di solito, i client e-mail sono applicazioni separate installate nel sistema dell'utente, ma alcuni prodotti (ad esempio, WorldClient Server di Alt-N Technologies) incorporano un client che viene "servito" al browser Web dell'utente. In questo modo, è possibile utilizzare come client i browser senza doverne installare uno nel computer. Ne risulta una maggiore portabilità e una migliore efficienza del sistema e-mail.

Crittografia - Si tratta di una misura di sicurezza basata sulla codifica delle informazioni di un file, che possono quindi essere lette solo se decodificate o decrittografate. La crittografia viene spesso utilizzata nella posta elettronica per impedire che un messaggio eventualmente intercettato da una terza parte possa essere letto. Il messaggio viene crittografato in fase di invio e decifrato al momento della ricezione.

Ethernet - Il tipo più diffuso di connessione utilizzata nelle LAN (Local Area Network). Le forme di Ethernet più usate sono 10BaseT e 100BaseT. Una connessione Ethernet 10BaseT è in grado di trasferire i dati a una velocità pari a 10 mbps (megabit al secondo) via cavo o connessione wireless (senza fili). Una connessione Ethernet 100BaseT trasferisce i dati a una velocità massima di 100 mbps. Una connessione Ethernet Gigabit è in grado di effettuare trasferimenti a una velocità pari a 1000 mbps ed è utilizzata da alcuni computer Apple.

ETRN - Acronimo di **E**xtended **TURN**. Si tratta di un'estensione al protocollo SMTP che consente a un server SMTP di inviare a un altro server SMTP, che ne conserva la posta, una richiesta di invio della posta, ossia di annullamento dell'accodamento dei messaggi. Poiché il solo SMTP non è in grado di richiedere la posta, generalmente richiesta mediante i protocolli POP e IMAP, il server SMTP che effettua la richiesta ETRN comunica al server remoto di avviare una sessione SMTP e di iniziare l'invio all'host specificato nella richiesta della posta memorizzata.

Il comando `TURN` utilizzato a tale scopo sollevava un rischio di sicurezza, poiché provocava l'inversione della direzione della sessione SMTP avviando immediatamente l'invio della posta memorizzata senza alcuna verifica o autenticazione dell'identità del server che emetteva la richiesta. `ETRN` avvia una nuova sessione SMTP anziché invertirne la direzione. In questo modo, se il server che emette la richiesta è un host "mascherato", il server di invio tenta comunque di consegnare la posta al vero host.

Attualmente, è in corso di valutazione la proposta di nuovo standard che prevede il comando Authenticated TURN (`ATRN`), il quale, analogamente a `TURN`, inverte la direzione della sessione SMTP ma, diversamente da TURN, richiede prima l'autenticazione. Lo standard in questione è ODMR (On-Demand Mail Relay). Il server MDaemon di Alt-N Technologies supporta sia il comando ETRN che il comando ATRN di ODMR.

Il sistema ETRN viene descritto nella RFC-1985, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc1985.txt

Il sistema ODMR viene descritto nella RFC-2645, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2645.txt

FAQ - Acronimo di "**F**requently **A**sked **Q**uestions". Si tratta di documenti in cui vengono raccolte le risposte alle domande sollevate più di frequente su un determinato argomento. Di solito vengono presentati in formato di elenco, in cui a ogni domanda segue la risposta corrispondente. Nelle FAQ più estese è probabile che tutte le domande vengano elencate all'inizio del documento con i riferimenti (o i collegamenti ipertestuali, nel caso delle FAQ su Internet) alla posizione di ciascuna coppia di domanda e risposta all'interno del documento. Le FAQ vengono spesso utilizzate prima di consultare il supporto tecnico e le istruzioni operative, in modo da risparmiare tempo.

File Transfer Protocol - Vedere FTP più avanti.

Firewall - Nella terminologia informatica, un *firewall* esiste quando si adottano delle misure di sicurezza (sia software che hardware) per suddividere una rete di computer in due o più parti o per limitarne l'accesso a determinati utenti. Ad esempio, è possibile consentire a chiunque di visualizzare la home page di un sito Web presente sulla rete ma autorizzare all'accesso ad alcune aree speciali solo specifici utenti. A prescindere dal metodo utilizzato (la richiesta di una password, la restrizione d'accesso per determinati indirizzi IP e così via), le aree speciali vengono definite "protette da firewall".

FTP - Acronimo di "**F**ile **T**ransfer **P**rotocol". Si tratta di un metodo particolarmente efficiente e alquanto diffuso per trasferire i file via Internet da un computer a un altro. A questo scopo, sono state sviluppate apposite applicazioni client/server, denominate "server FTP" e "client FTP" (due dei client più diffusi sono FTP Voyager e CuteFTP). Di solito, i client FTP sono in grado di eseguire diverse altre funzioni oltre al semplice trasferimento dei file. Inoltre, alcuni browser Web includono il supporto per il File Transfer Protocol, benché talvolta tale supporto consenta solo lo scaricamento. In aggiunta, alcuni server FTP sono di tipo "anonymous" (anonimo), il che significa che chiunque può accedervi per scaricare i file, solitamente specificando "anonymous" come nome utente e il proprio indirizzo e-mail come password. Spesso, i siti FTP anonimi consentono di scaricare i file senza che l'utente esegua l'accesso: è sufficiente fare clic su un collegamento. Per i browser che supportano l'FTP, di solito è sufficiente connettersi al sito FTP specificando "ftp://…" anziché "http://…" nell'URL.

Il protocollo FTP viene descritto nella RFC-959, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc959.txt

Gateway - Componente hardware o software che converte i dati tra due applicazioni o reti dotate di protocolli diversi. Il termine "gateway" viene utilizzato anche per indicare qualsiasi metodo che consente di accedere da un sistema a un altro. Ad esempio, il provider di servizi Internet è un gateway per Internet.

Grazie alla funzionalità Gateway di dominio, il server e-mail MDaemon di Alt-N Technologies può fungere da gateway e-mail per altri domini. Opera come intermediario, o gateway, raccogliendo la posta di un dominio e conservandola finché il dominio in questione non provvede a ritirarla. Si tratta di una funzione utile sia per i domini che non mantengono una connessione continua a Internet, sia per i domini che richiedono un server di backup nel caso il proprio sia soggetto a guasti.

GIF - Acronimo di "**G**raphics **I**nterchange **F**ormat". Si tratta del formato per i file di immagine più utilizzato su Internet. I file GIF utilizzano i colori indicizzati o una tavolozza composta da un determinato numero di colori, così che le dimensioni risultano estremamente ridotte, soprattutto quando l'immagine contiene grandi aree dello stesso colore. La dimensione ridotta velocizza il trasferimento dei file di immagine tra i sistemi e rende questo formato molto popolare su Internet. Poiché la formula di compressione GIF è stata originariamente sviluppata da CompuServe, spesso le immagini GIF vengono indicate come CompuServe GIF.

Interfaccia grafica utente - Vedere GUI.

GUI - Acronimo di "**G**raphical **U**ser **I**nterface" (Interfaccia grafica utente). La GUI rende possibile l'interazione con il computer o un'applicazione poiché impiega un dispositivo di puntamento per selezionare gli elementi grafici sullo schermo anziché richiedere di digitare del testo nella riga di comando. I sistemi operativi Microsoft Windows e Apple Mac sono entrambi basati su GUI, ma, benché introdotto originariamente da Apple, il concetto di interfaccia utente grafica è stato sviluppato da Xerox.

Host - Qualunque computer in rete che funge da server per gli altri computer della stessa rete. Il sistema host può essere eseguito come server Web, come server di posta o come servizio di altro tipo. Di norma, fornisce più servizi contemporaneamente.

Nelle reti peer-to-peer è frequente che i sistemi siano contemporaneamente host e client. Ad esempio, un sistema può fungere da host per la stampante di rete ed essere simultaneamente utilizzato come client per raccogliere la posta e scaricare i file da un altro host.

HTML Acronimo di "**H**ypertext **M**arkup **L**anguage". Si tratta del linguaggio di codifica utilizzato per creare i documenti ipertestuali presenti sul World Wide Web. In termini più semplici, un documento HTML è un documento di testo semplice che contiene dei codici e dei tag di formattazione. Questi vengono interpretati dal browser Web, che presenta agli utenti una pagina Web completa di colori e testo formattato. Ad esempio, un browser che riceve un documento HTML contenente il testo "<B>Testo</B>" visualizza il termine "Testo" in grassetto. Poiché hanno dimensioni molto ridotte, i file di testo semplice possono essere trasferiti su Internet piuttosto velocemente.

HTTP - Acronimo di **H**ypertext **T**ransfer **P**rotocol. Si tratta del protocollo utilizzato per trasferire i file *ipertestuali* tra i computer collegati a Internet. Il protocollo HTTP richiede un programma client a un'estremità (di solito, un browser Web) e un server HTTP all'altra.

Il protocollo FTP viene descritto nella RFC-2616, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2616.txt

Ipertesto - Qualunque testo contenente un collegamento ipertestuale a un altro documento o a un altro punto dello stesso documento. Talvolta, il testo viene definito collegamento ipertestuale, collegamento o link. L'ipertesto può essere costituito da una parola o da una frase e incorpora il collegamento in modo che, facendo clic su di esso, l'utente può spostarsi in corrispondenza del punto "contrassegnato" o visualizzare il documento collegato. Di solito, i collegamenti ipertestuali sono evidenti perché il testo è sottolineato e di colore diverso, anche se questo non è obbligatorio. In alcuni casi, l'ipertesto non presenta un aspetto diverso dal testo normale, ma in genere risulta distinguibile dalla variazione grafica del puntatore che consegue dal posizionamento del mouse sul testo che funge da collegamento.

Hypertext Markup Language - Vedere HTML.

IMAP - Sviluppato dall'università di Stanford, il protocollo IMAP, **I**nternet **M**essage **A** ccess **P**rotocol viene utilizzato per gestire e recuperare i messaggi e-mail. La versione più recente è IMAP4 ed è simile a POP3, pur includendo una serie di caratteristiche aggiuntive. IMAP4 è particolarmente conosciuto come protocollo utilizzato per gestire la posta sul server anziché sul sistema locale dell'utente: i messaggi possono essere cercati in base alle parole chiave, organizzati in cartelle e specificamente selezionati per essere scaricati o per consentire altre funzioni mentre si trovano ancora sul server. Il protocollo IMAP risulta meno impegnativo per il sistema dell'utente. Inoltre, centralizza la posta elettronica, consentendo così di accedervi da posizioni diverse.

Il protocollo IMAP viene descritto nella RFC-2060, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2060.txt

Estensione IMAP4 ACL - Vedere ACL.

Internet - Internet è stata creata nel 1969 dall'esercito degli Stati Uniti, originariamente come rete di comunicazione indistruttibile in caso di conflitto nucleare. Oggi è costituita da milioni di computer e reti in tutto il mondo. Internet è decentralizzata, ovvero non è controllata da alcuna azienda, organizzazione o nazione. Ciascun host (o computer) su Internet è indipendente dagli altri ed è in grado di fornire qualsiasi informazione o servizio reso disponibile dai propri operatori. Ciononostante, la maggior parte delle informazioni trasferite su Internet in qualche punto passa attraverso delle "dorsali", connessioni a larga banda e ad alta velocità, controllate dai maggiori provider e dalle maggiori organizzazioni. La maggior parte degli utenti accede a Internet attraverso un servizio online come AOL o per mezzo di un provider di servizi Internet (ISP, Internet Service Provider), che gestisce o si connette a una di queste dorsali.

Molti credono che il *World Wide Web* (WWW) e Internet siano la stessa cosa, ma non è così. Il World Wide Web è solo una parte di Internet. Si tratta della parte di Internet più visibile e conosciuta, generalmente gestita e strutturata in base a dettati commerciali, ma non coincide con l'interezza di Internet.

Intranet - In termini semplici, un'intranet è una piccola Internet privata utilizzata solo all'interno della rete di un'azienda o di un'organizzazione. Benché varino sensibilmente da un'organizzazione all'altra, le intranet possono integrare qualunque funzione disponibile su Internet. Possono ad esempio includere sistemi e-mail, directory di file, pagine Web da consultare, articoli da leggere e così via. La differenza principale tra un'intranet e Internet risiede nel fatto che un'intranet è relativamente piccola e comunque confinata a un'organizzazione o un gruppo.

IP - Acronimo di "**I**nternet **P**rotocol", come in TCP/IP. I protocolli Internet rendono possibile il trasferimento dei dati tra i diversi sistemi connessi a Internet. A prescindere dalla piattaforma o dal sistema operativo di ciascun sistema, se lo stesso protocollo Internet viene utilizzato da tutti i sistemi, questi sono in grado di scambiarsi dati. Il termine "IP" viene spesso utilizzato come ulteriore abbreviazione di "indirizzo IP". Il protocollo Internet standard corrente è IP versione 4 (IPv4).

Il protocollo Internet viene descritto nella RFC-791, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc791.txt

Indirizzo IP - Talvolta definito anche numero IP, l'indirizzo IP (**I**nternet **P**rotocol) viene utilizzato per identificare una specifica rete TCP/IP e gli host o i sistemi che la compongono. Si tratta di un indirizzo numerico a 32 bit contenente quattro numeri compresi tra 0 e 255, separati da punti, ad esempio "127.0.0.1". All'interno di una rete isolata, ciascun nome di computer deve avere un indirizzo IP univoco, a volte assegnato in modo casuale. In Internet ogni computer deve invece disporre di un indirizzo IP registrato per evitare duplicazioni. Gli indirizzi IP di Internet possono essere statici o dinamici. I primi non cambiano e rappresentano sempre la stessa posizione o lo stesso sistema su Internet. I secondi cambiano e vengono solitamente assegnati da un ISP a quei computer che si trovano su Internet solo temporaneamente (ad esempio, quando un utente accede a Internet mediante un account di accesso remoto). Tuttavia, è possibile che a un account di accesso remoto venga assegnato un indirizzo IP statico.

I provider e le grandi organizzazioni cercano di solito di acquisire una gamma o un set di indirizzi IP dall'InterNIC Registration Service, in modo che tutti i client o gli utenti delle proprie reti abbiano indirizzi simili. Questi set vengono suddivisi in tre classi: A, B e C. I set di classe A e B vengono utilizzati dalle organizzazioni molto grandi e supportano rispettivamente 16.000.000 e 65.000 host. I set di classe C sono destinati alle reti più piccole e supportano 255 host. Poiché i set di classe A e B sono oggi molto difficili da ottenere a causa della scarsità di indirizzi disponibili, gran parte delle aziende devono accontentarsi dei set di classe C. A causa di questa scarsità di indirizzi IP, un nuovo protocollo per gli indirizzi IP, denominato CIDR (Classless Inter-domain Routing), sta gradualmente sostituendo quello classico.

Il protocollo Internet standard corrente, Ipv4, viene descritto nella RFC-791, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc791.txt

Il protocollo Internet versione 6 (IPv6) viene descritto nella RFC-2460, consultabile all'indirizzo

http://www.rfc-editor.org/rfc/rfc2460.txt

Il protocollo CIDR viene descritto nelle RFC 1517-1519, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc1517.txt

http://www.rfc-editor.org/rfc/rfc1518.txt

http://www.rfc-editor.org/rfc/rfc1519.txt

Numero IP - Vedere *Indirizzo IP*.

ISP - **I**nternet **S**ervice **P**rovider (Provider di servizi Internet). L'ISP, o più comunemente il provider, è un'azienda che fornisce accesso e servizi Internet agli utenti finali. La maggior parte degli ISP fornisce ai propri clienti più servizi Internet, ad esempio l'accesso al World Wide Web, la posta elettronica, l'accesso ai newsgroup e ai server news e così via. In genere, gli utenti si collegano all'ISP mediante una connessione di accesso remoto o di altro tipo. Successivamente, l'ISP collega gli utenti a un router, che a sua volta li instrada alla dorsale Internet.

Java - Sviluppato da Sun Microsystems, Java è un linguaggio di programmazione orientato alle reti con una sintassi molto simile a quella di C/C++, ma strutturata sulle classi anziché sulle funzioni. Nelle applicazioni Internet viene comunemente utilizzato per programmare le applet, ovvero i piccoli programmi incorporati nelle pagine Web. Questi programmi possono essere automaticamente scaricati ed eseguiti dal browser di un utente al fine di fornire una vasta gamma di funzioni, che non sarebbero possibili con l'utilizzo del semplice HTML o di altri linguaggi di script, e senza il rischio di infezioni da virus o danni al computer. Poiché Java è sia efficiente che facile da utilizzare, sta diventando molto popolare tra gli sviluppatori software e hardware.

JavaScript - Da non confondersi con Java. JavaScript è stato sviluppato da Netscape come linguaggio di script progettato per estendere le capacità dell'HTML e creare pagine Web interattive. Si tratta di un linguaggio di programmazione semplificato, più facile da utilizzare rispetto a Java e ad altri linguaggi, ma anche più limitato. Nonostante i limiti, si rivela molto utile per aggiungere elementi interattivi ai siti Web. Ad esempio, JavaScript può essere efficientemente utilizzato quando si desidera che i dati vengano pre-elaborati prima di essere inviati al server oppure che le pagine rispondano all'interazione da parte dell'utente con collegamenti o altri elementi di forma. Può inoltre essere utilizzato per controllare i plug-in e le applet che si basano sulle selezioni dell'utente, nonché per eseguire numerose altre funzioni. JavaScript è incluso nel testo dei documenti HTML e, affinché le funzioni vengano eseguite, deve essere interpretato dai browser Web.

JPEG - Formato di file grafico più efficiente del GIF nella compressione delle immagini a 65.536 colori e di quelle fotografiche. Mentre il formato GIF rappresenta la soluzione ottimale per le immagini contenenti forme regolari e grandi aree di motivi di

colore ripetuti, il JPEG risulta più adatto per le immagini con motivi irregolari e grandi quantità di colori. JPEG è il formato più utilizzato per le immagini a 65.536 colori e le immagini fotografiche su Internet. È l'acronimo di "**J**oint **P**hotographic **E**xperts **G** roup", il gruppo che ha sviluppato il formato.

Kbps - Unità di misura utilizzata comunemente per le velocità dei modem (ad esempio, 56 Kbps). È l'acronimo di "**K**ilo**b**its **P**er **S**econd (kilobit al secondo)". Misura la quantità di kilobit (1000 bit) di dati che vengono spostati o elaborati ogni secondo. Si noti che si tratta di *kilobit* e non di *kilobyte*: la dimensione di un kilobyte è infatti otto volte quella di un kilobit.

Kilobyte - Un kilobyte (abbreviato in K o KB) corrisponde a mille byte di dati. Tecnicamente, equivale a 1024 byte (2^10 = 1024), tuttavia nell'uso comune viene solitamente approssimato a 1000.

LAN - Una LAN (**L**ocal **A**rea **N**etwork) è una rete di computer limitata a un singolo edificio o area, i cui nodi (computer o workstation) sono di solito connessi l'uno con l'altro con una configurazione di fili, cavi o altri tipi di supporto. La maggior parte delle grandi aziende dispone di reti LAN, poiché semplificano considerevolmente la gestione e la condivisione delle informazioni tra i dipendenti e gli uffici. La maggior parte delle reti LAN utilizza un sistema e-mail o chat e condivide i dispositivi, ad esempio le stampanti, che non devono pertanto essere installati in ogni stazione. Quando i nodi della rete sono connessi mediante linee telefoniche, onde radio o collegamenti satellitari, la LAN viene definita WAN (Wide Area Network).

Latenza - Tempo impiegato da un pacchetto di dati per spostarsi lungo una connessione di rete. Mentre un pacchetto di dati viene inviato, si sviluppa un tempo "latente" durante il quale il computer mittente attende conferma dell'avvenuta ricezione del pacchetto. Insieme alla larghezza di banda, la latenza è uno dei fattori che determinano la velocità di una connessione.

LDAP - Acronimo di **L**ightweight **D**irectory **A**ccess **P**rotocol. Si tratta di una versione semplificata del protocollo per servizi di elenchi in linea DAP (Directory Access Protocol). Il sistema di directory è una struttura gerarchica composta dai livelli seguenti: la directory principale o iniziale, il Paese, l'organizzazione, l'unità organizzativa e l'individuo all'interno dell'unità. Ogni voce LDAP è una raccolta di attributi con un identificatore univoco, definito DN (Distinguished Name). Poiché si tratta di un protocollo aperto e distribuibile su più server, LDAP può in ultima analisi consentire a qualunque applicazione o piattaforma in qualunque parte del mondo di accedere alle informazioni dell'elenco in linea per individuare gli indirizzi e-mail, le organizzazioni, i file e così via.

Il protocollo LDAP viene descritto nella RFC-2251, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2251.txt

Link - Vedere *Ipertesto*.

Server list - Applicazione server utilizzata per distribuire i messaggi e-mail a più destinatari specificando un solo indirizzo. In termini semplici, quando viene indirizzato a una *lista di distribuzione* gestita dal server list, un messaggio e-mail viene automaticamente trasmesso a tutti i membri della lista. Le liste di distribuzione

hanno di solito un solo indirizzo e-mail normale (ad esempio, nomelista@esempio.com), che fa riferimento a un intero elenco di destinatari anziché a una persona o a una casella postale specifica. Quando un utente *si iscrive* a una lista di distribuzione, il server list ne aggiunge automaticamente l'indirizzo alla lista e distribuisce i futuri messaggi diretti alla lista a tale indirizzo (o membro) e a tutti gli altri. Quando un utente annulla l'iscrizione, il server list semplicemente rimuove l'indirizzo, in modo che non riceva più messaggi di lista.

Spesso, il termine "listserv" viene genericamente usato per indicare il server di una lista di distribuzione. Tuttavia, Listserv® è un marchio registrato di L-Soft international, Inc. ed è un vero e proprio programma sviluppato da Eric Thomas per BITNET nel 1986. Tra gli altri server list, il server MDaemon di Alt-N Technologies è dotato di un'intera suite di caratteristiche e funzioni da server list o di gestione delle liste di distribuzione.

Logon - Codice univoco o serie di caratteri da utilizzare per ottenere l'accesso o identificarsi presso un server o un computer. Nella maggior parte dei casi, l'accesso viene consentito solo se al nome di logon viene associata una password.

Esistono numerosi sinonimi di "logon", ad esempio login, nome utente o ID utente.

Casella postale - Area della memoria o di un dispositivo di memorizzazione assegnata a uno specifico indirizzo e-mail, in cui vengono archiviati i messaggi e-mail. A prescindere dal tipo di sistema e-mail in uso, ciascun utente dispone di una casella postale privata in cui vengono memorizzati i messaggi man mano che il server di posta li riceve. Il termine "casella postale" viene spesso utilizzato per indicare la porzione alla destra di un indirizzo e-mail. In "", ad esempio, "Franco" rappresenta la casella di posta, mentre "altn.com" è il nome di dominio.

Lista di distribuzione - Definita anche gruppo e-mail, la lista di distribuzione è un elenco o un gruppo di indirizzi e-mail identificati da un unico indirizzo e-mail, ad esempio "nomelista@esempio.com". Di solito, quando un server list riceve un messaggio e-mail indirizzato a una delle proprie liste di distribuzione, il messaggio viene automaticamente distribuito a tutti i membri della lista, ovvero agli indirizzi inclusi nell'elenco. Il server MDaemon di Alt-N Technologies è dotato di una vasta gamma di funzioni di gestione delle liste di distribuzione che possono essere utilizzate per rendere le liste pubbliche o private (l'invio dei messaggi è aperto a chiunque o riservato ai soli membri) oppure moderate (ogni messaggio deve essere approvato da qualcuno prima di essere inviato alla lista), nonché per inviarle in formato riassunto o come messaggi singoli.

Megabyte - Benché dal punto di vista tecnico corrisponda a 1.048.576 byte (o 1024 kilobyte), un megabyte è generalmente approssimato a un milione di byte. Megabyte è abbreviato in "MB", come in "20 MB".

MIME - Definito nel 1992 dalla Internet Engineering Task Force (IETF), il MIME (**M**ultipurpose **I**nternet **M**ail **E**xtensions) è un metodo di codifica standard utilizzato per allegare i file non testuali ai messaggi e-mail standard. Poiché di solito solo i file di testo semplice possono essere trasferiti via e-mail, i file non testuali devono essere dapprima codificati in formato di testo semplice, quindi decodificati una volta raggiunta la propria destinazione. Pertanto, un programma e-mail viene considerato compatibile con MIME se invia e riceve i file mediante lo standard MIME. Quando viene inviato un allegato con codifica MIME, come parte del messaggio vengono di

solito specificati sia il tipo di file inviato che il metodo da utilizzare per ripristinarne la forma originale. Esistono molti tipi di contenuto MIME predefiniti, ad esempio "image/jpeg" e "text/plain". È tuttavia possibile definire anche dei tipi MIME personalizzati.

Lo standard MIME viene utilizzato anche dai server Web per identificare i file inviati ai browser Web. Poiché supportano vari tipi di MIME, i browser Web sono in grado di visualizzare o produrre file in formato non HTML. Inoltre, aggiornando gli elenchi MIME-Types dei browser e del software utilizzato per la gestione di ciascun tipo, è possibile supportare immediatamente nuovi formati di file.

Il sistema MIME viene descritto nelle RFC 2045-2049, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc2045.txt

http://www.rfc-editor.org/rfc/rfc2046.txt

http://www.rfc-editor.org/rfc/rfc2047.txt

http://www.rfc-editor.org/rfc/rfc2048.txt

http://www.rfc-editor.org/rfc/rfc2049.txt

Mirror - Server, di solito di tipo FTP, in cui è contenuta una copia dei file presenti su un altro server. Viene in genere utilizzato per fornire una posizione alternativa da cui scaricare i file, se il server originale diventa indisponibile. Il termine "mirror" (specchio) fa anche riferimento a una configurazione in cui le informazioni vengono scritte su più dischi fissi contemporaneamente . Di norma, tale configurazione viene utilizzata come misura di ridondanza per consentire il funzionamento del sistema e impedire la perdita di dati importanti nel caso si verifichi un guasto in uno dei dischi.

Modem - Acronimo derivato da **mo**dulator-**dem**odulator. Si tratta di un dispositivo connesso a un computer che consente di trasferire dati ad altri computer tramite le linee telefoniche. Il modem converte in formato analogico (modulazione) i dati digitali del computer e successivamente li trasferisce a un altro modem, che esegue l'operazione inversa (demodulazione). In altri termini, il modem è un convertitore da analogo a digitale e viceversa. La velocità con cui vengono trasferiti i dati viene espressa sia in termini di velocità in baud, ad esempio 9.600 baud, sia in termini di kilobit al secondo, ad esempio 28,8 kbps.

MultiPOP - Componente del server di posta MDaemon di Alt-N Technologies. Può essere configurato per raccogliere la posta con il protocollo POP3, contemporaneamente a diversi server e-mail, per conto degli utenti di MDaemon. In questo modo, i titolari degli account di MDaemon provvisti di altri account e-mail su server e-mail diversi possono raccogliere la posta con l'e-mail dell'account di MDaemon e memorizzare quindi tutti i messaggi in una sola casella postale.

NAT - Acronimo di Network Address Translation. Vedere Conversione degli indirizzi di rete più avanti.

Rete - Due o più computer connessi tra loro. Una rete viene appositamente progettata per consentire la condivisione di risorse e di informazioni tra più sistemi. Ne sono esempi significativi i sistemi composti da più computer che condividono

stampanti, unità DVD-ROM o dischi fissi.

Esistono molti tipi di rete, ma le più diffuse sono le LAN (Local Area Network) e le WAN (Wide Area Network). In una LAN, i singoli computer (detti nodi) sono vicini geograficamente, spesso nello stesso edificio. Inoltre, sono solitamente connessi direttamente mediante cavi, benché ultimamente si stiano affermando anche le connessioni senza fili. I nodi di una WAN sono di solito più lontani (ubicati in edifici o città diverse) e connessi mediante linee telefoniche, collegamenti satellitari o altri mezzi.

Internet è una rete, spesso indicata come rete di reti.

Conversione degli indirizzi di rete - Definita anche NAT (Network Address Translation). Si tratta di un sistema che consente a un'unica rete di utilizzare due set di indirizzi IP: uno per il traffico esterno e uno per quello interno. Questo tipo di sistema viene principalmente utilizzato come firewall per la sicurezza della rete. Il computer di un utente mostra ai computer esterni alla LAN un determinato indirizzo IP, mentre l'indirizzo IP effettivo è completamente diverso. I sistemi hardware o software posti tra la rete e Internet eseguono le conversioni tra i due indirizzi. Grazie a questo metodo, è probabile che più computer in una LAN possano condividere un unico indirizzo IP aziendale. In questo modo, nessuno al di fuori della rete è in grado di conoscere l'indirizzo del computer di un utente o collegarvisi se non è stato autorizzato o autenticato durante la conversione.

Scheda di interfaccia di rete - Definita anche NIC (Network Interface Card). Si tratta di una scheda a circuito che consente a un computer di collegarsi a una rete. Le schede NIC forniscono connessioni di rete permanenti, mentre i modem (utilizzati per collegare in rete con accesso remoto gran parte dei computer domestici) forniscono di solito solo connessioni temporanee. La maggior parte delle schede NIC è progettata per tipi specifici di reti e protocolli, quali Ethernet o Token Ring e TCP/IP.

Network News Transfer Protocol - Vedere NNTP più avanti.

NIC - Acronimo di Network Interface Card. Vedere Scheda di interfaccia di rete.

NNTP - Acronimo di **N**etwork **N**ews **T**ransfer **P**rotocol. Si tratta del protocollo utilizzato per trasferire e distribuire i messaggi nei newsgroup USENET. I browser e i client e-mail più diffusi incorporano client NNTP.

Il sistema NNTP viene descritto nella RFC-977, consultabile su Internet all'indirizzo

`http://www.rfc-editor.org/rfc/rfc977.txt`

Nodo - Qualunque computer singolo connesso a una rete.

ODMR - Acronimo di **O**n-**D**emand **M**ail **R**elay. Si tratta del nuovo protocollo progettato per consentire ai server di posta dotati solo di una connessione intermittente a un provider e che non dispongono di un indirizzo IP statico di ricevere la posta in modo simile ai server dotati di indirizzo IP statico e che utilizzano il comando `ETRN`. Se il sistema è dotato di indirizzo IP statico, è possibile utilizzare il comando ESMTP ETRN. Tuttavia, i sistemi sprovvisti di indirizzi IP dinamici non dispongono di una soluzione efficace. ODMR risolve questo inconveniente. Tra gli altri, il protocollo ODMR introduce il comando Authenticated TURN (`ATRN`), che

provoca l'inversione del flusso di una sessione SMTP (in modo simile al precedente comando TURN) ma fornite di una richiesta di autenticazione da parte del server richiedente. In questo modo, un server SMTP con un indirizzo IP dinamico è in grado di connettersi al proprio ISP e ricevere la posta di uno o più host mediante SMTP anziché raccoglierla mediante POP o IMAP. In questo modo, è possibile fornire una soluzione a basso costo alle aziende che richiedono un server proprietario, ma non possono permettersi un indirizzo IP statico o una presenza online dedicata.

Il sistema ODMR viene descritto nella RFC-2645, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2645.txt

OEM - Acronimo di **O**riginal **E**quipment **M**anufacturer. Si tratta di un termine spesso confuso e frainteso. Un OEM è un'azienda che utilizza l'attrezzatura o i prodotti di un'altra azienda nei propri prodotti, confezionati e venduti con un marchio o un nome aziendale diverso. Ad esempio, HyperMegaGlobalCom, Inc. è un OEM, poiché acquista componenti di computer da uno o più produttori diversi, li assembla in un unico prodotto personalizzato e li rivende sotto il marchio "HyperMegaGlobalCom". L'azienda che ha venduto i propri componenti a HyperMegaGlobalCom può essere anch'essa un OEM, se a sua volta ha acquistato i componenti da un altro produttore. Il termine "OEM" è utilizzato spesso in modo improprio, perché gli OEM non sono in realtà i produttori originali, bensì le aziende che "personalizzano" il software o lo incorporano nei propri prodotti. Ciononostante, il termine "OEM" viene spesso utilizzato per fare riferimento ai produttori hardware.

Al volo - Il termine "al volo" (talvolta anche "on the fly") ha di solito due significati. Nel primo caso, indica un'operazione che può essere effettuata "di fretta" o facilmente durante l'esecuzione di un'altra operazione. Ad esempio, un prodotto per la creazione dei segnalibri può supportare la creazione di account "al volo" durante l'immissione di cifre relative alle vendite, come "Interrompere l'immissione delle cifre, fare clic sul pulsante X, immettere un nome, quindi continuare con l'immissione di altre cifre". Un'operazione viene definita "al volo" anche quando può essere generata dinamicamente o automaticamente anziché manualmente o staticamente. Ad esempio, utilizzando le informazioni memorizzate in un "cookie", è possibile generare "al volo" una pagina Web personalizzata, non appena un utente accede di nuovo a un sito Web. Anziché richiedere la creazione manuale di una pagina personalizzata in base ai gusti dell'utente, la pagina viene generata dinamicamente in base alle operazioni eseguite dall'utente durante la navigazione.

Original Equipment Manufacturer - Vedere OEM.

Pacchetto - Unità di dati informatici inviati su una rete. I dati che si ricevono da un altro computer connesso alla LAN o a Internet hanno la forma di "pacchetti". Il file o il messaggio originale viene dapprima suddiviso in pacchetti, quindi trasmesso e infine ricombinato, quando raggiunge la destinazione finale. Ogni pacchetto include un'intestazione contenente l'origine e la destinazione, un blocco di dati e un codice di verifica degli errori. Al pacchetto viene inoltre assegnato un numero, con cui è possibile collegarlo ai pacchetti correlati inviati. Il processo di invio e ricezione dei pacchetti è noto come "commutazione di pacchetto". I pacchetti sono denominati anche "datagrammi".

Commutazione di pacchetto - Processo di invio e ricezione di pacchetti su una rete o su Internet. A differenza della commutazione di circuito, ad esempio quella dei

telefoni analogici, che invia i dati con un flusso continuo su un singolo percorso o circuito, la commutazione di pacchetto trasmette i dati suddividendoli in "pacchetti", che non seguono necessariamente lo stesso percorso per giungere a destinazione. Inoltre, poiché i dati sono in unità separate, più utenti possono contemporaneamente inviare file diversi sullo stesso percorso.

Parametro - Un parametro è una caratteristica o un valore. In termini di elaborazione, rappresenta qualunque valore che viene passato a un programma da un utente o da un altro programma. Sono parametri i nomi, le password, le impostazioni, le dimensioni dei font e così via. In termini di programmazione, un parametro è un valore che viene passato a una subroutine o a una funzione per l'elaborazione.

PDF - Acronimo di **P**ortable **D**ocument **F**ormat. Si tratta di un formato di file multi-piattaforma a elevata compressione sviluppato da Adobe Systems Incorporated, in grado di catturare la formattazione, il testo e le immagini dei documenti creati con una vasta gamma di applicazioni. Diversamente da molti elaboratori di testo, consente di ottenere una visualizzazione e una stampa fedeli di un documento su più computer e piattaforme diverse. La visualizzazione dei file PDF richiede Adobe Acrobat Reader, un'applicazione distribuita gratuitamente da Adobe Systems. È comunque disponibile anche un plug-in che consente di visualizzare i file PDF direttamente nel browser Web. Il plug-in consente di visualizzare i file PDF pubblicati su un sito Web in modo diretto, senza che sia necessario scaricarli e aprirli con un programma separato.

Analisi sintattica - In campo linguistico, l'analisi sintattica è la suddivisione di una struttura linguistica nei suoi componenti grammaticali, ad esempio verbi, aggettivi e sostantivi.

In informatica, per analisi sintattica (o "parsing") si intende la suddivisione di un'istruzione in parti che possono rivelarsi utili per il computer. Un analizzatore sintattico (o "parser") di un compilatore suddivide ciascuna istruzione scritta da uno sviluppatore in parti che possono essere utilizzate per sviluppare ulteriori operazioni o per creare le istruzioni che compongono un programma eseguibile.

Il server MDaemon e altri prodotti di Alt-N Technologies effettuano spesso l'analisi sintattica dei messaggi e-mail per determinarne la destinazione o per elaborarli mediante filtri e altri strumenti.

Ping - Acronimo di **P**acket **In**ternet **G**roper. Si tratta di un programma Internet di base che determina se un determinato indirizzo IP è raggiungibile e accetta le richieste. Questa analisi viene eseguita inviando una richiesta ECHO ICMP (Internet Control Message Protocol) a cui deve seguire una risposta. Per eseguire il "ping" di un indirizzo IP, è sufficiente digitare "ping" seguito dall'indirizzo IP o dal dominio sul prompt dei comandi DOS, ad esempio "Ping 1.2.3.4".

I protocolli ICMP ed Echo vengono descritti rispettivamente nella RFC-792 e nella RFC-862, consultabili su Internet agli indirizzi:

http://www.rfc-editor.org/rfc/rfc792.txt

http://www.rfc-editor.org/rfc/rfc862.txt

POP - Acronimo di **P**ost **O**ffice **P**rotocol. Il protocollo POP (spesso indicato anche come POP3) è il protocollo e-mail più utilizzato per ritirare i messaggi da un server e-mail. La maggior parte dei client e-mail utilizza il protocollo POP, benché alcuni supportino anche il più recente protocollo IMAP. POP2, diventato uno standard verso la metà degli anni Ottanta, richiedeva SMTP per l'invio dei messaggi. La versione con cui è stato sostituito, ovvero POP3, può essere utilizzata anche senza SMTP.

Il protocollo POP3 viene descritto nella RFC-1939, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc1939.txt

Porta - Nella reti TCP/IP e UDP e su Internet, la porta costituisce il punto finale di una connessione logica ed è identificata da un numero compreso tra 0 e 65536. Le porte da 0 a 1024 sono riservate per alcuni protocolli e servizi privilegiati. Di solito, i server Web sono presenti sulla porta 80, i server SMTP comunicano mediante la porta 25 e i server POP inviano e ricevono la posta mediante la porta 25. In genere, una determinata porta su ciascun sistema può essere utilizzata da un solo programma alla volta. Quando si naviga in Internet, è probabile che alcuni server vengano eseguiti su porte non predefinite. In questi casi, è necessario specificare la porta nell'URL, preceduta da un segno di due punti. Ad esempio, "www.esempio.com:3000".

Una porta può essere utilizzata anche per fare riferimento ai socket di un computer utilizzato per la connessione di periferiche e altri dispositivi hardware, ad esempio porte seriali, porte parallele o porte USB.

Infine, il concetto di porting (in inglese, "to port") viene spesso impiegato per descrivere il processo in base al quale un programma progettato per una piattaforma specifica viene eseguito su un'altra piattaforma.

Post - Nella messaggistica Internet, indica un singolo messaggio immesso nel sistema di comunicazione di rete per essere condiviso, ad esempio un messaggio visualizzato in un newsgroup, in una lista di distribuzione o in un forum.

PPP - Acronimo di "Point to Point Protocol". Si tratta dello standard Internet per le connessioni di accesso remoto. PPP è un set di regole che definisce il modo in cui la connessione via modem scambia i pacchetti di dati con gli altri sistemi su Internet.

Il protocollo PPP viene descritto nella RFC-1661, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc1661.txt

Protocollo - In informatica, un protocollo è costituito da un set di indicazioni o standard in base a cui comunicano i server e le applicazioni. Esistono numerosi tipi di protocollo, utilizzati per scopi diversi: TCP/IP, SLIP, HTTP, POP3, SMTP, IMAP, FTP e così via.

Registro - Database utilizzato da Microsoft Windows per memorizzare le informazioni di configurazione relative al software installato nel computer, ad esempio le impostazioni personalizzate, le associazione delle estensioni dei file, gli sfondi del desktop, gli schemi colori e così via. Il registro è suddiviso nelle seguenti parti:

HKEY_User - Memorizza le informazioni relative a ciascun utente del sistema.

HKEY_Current_User - Memorizza le preferenze dell'utente corrente.

HKEY_Current_Configuration - Memorizza le impostazioni dello schermo e delle stampanti.

HKEY_Classes_Root - Include le associazioni dei file e le informazioni OLE.

HKEY_Local_Machine - Memorizza le impostazioni per l'hardware, il sistema operativo e le applicazioni installate.

HKEY_Dyn_Data - Include i dati relativi alle prestazioni.

Quando si installano dei programmi nel computer, il programma di installazione scrive automaticamente alcune informazioni nel registro. Anche se il registro può essere modificato manualmente, è preferibile utilizzare il programma regedit.exe fornito da Windows. Si consiglia di eseguire questa operazione con attenzione perché la modifica non corretta di un'impostazione può dare origine a gravi malfunzionamenti del computer.

RFC - Acronimo di **R**equest **F**or **C**omments . Si tratta del nome assegnato al processo di creazione di uno standard su Internet e al relativo risultato. Ogni nuovo standard o protocollo viene proposto e pubblicato su Internet sotto forma di "Request For Comments" (Richiesta di commenti). L'IETF (Internet Engineering Task Force) promuove il dibattito sul nuovo standard, che diventa ufficiale solo successivamente. Anche quando è perfettamente definito e non vengono più richiesti commenti, lo standard conserva l'acronimo RCF insieme al numero di identificazione. Ad esempio, RFC-822 (ora sostituito da RFC-2822) è lo standard ufficiale, o RFC, per l'e-mail. Tuttavia, ai protocolli ufficialmente adottati come "standard" è comunque associato un numero standard ufficiale, riprodotto nel documento Internet Official Protocol Standards (il quale è a sua volta indicato come STD-1 e, correntemente, come RFC-3700). Le RCF sono disponibili su Internet in diversi punti, ma l'origine ufficiale è "RFC Editor", all'indirizzo http://www.rfc-editor.org/.

Il documento Internet Official Protocol Standards è consultabile all'indirizzo:

http://www.rfc-editor.org/rfc/std/std1.txt

RTF - Acronimo di **R**ich **T**ext **F**ormat . Si tratta di un formato di file universale sviluppato da Microsoft e supportato da quasi tutti gli elaboratori di testo. A differenza del formato di testo semplice, il formato RTF consente di conservare la formattazione, le informazioni sui font, il colore del testo e così via. La dimensione dei file RTF può essere molto superiore a quella di altri formati, quali il formato di documento di Word 2000 (*.doc) e Adobe PDF.

Server - Computer o programma che fornisce uno specifico tipo di servizio al software client in esecuzione su altri computer. Il termine può fare riferimento a un particolare software, ad esempio un server SMTP, oppure a un sistema su cui quel software viene eseguito. Su un singolo *sistema* server possono essere in esecuzione più *programmi* server. Ad esempio, sul server di una rete possono essere contemporaneamente in esecuzione un server Web, un server e-mail, un server FTP, un server fax e altri ancora.

SMTP - Acronimo di **S**imple **M**ail **T**ransfer **P**rotocol. Si tratta del protocollo principale utilizzato per inviare la posta elettronica su Internet da un server all'altro o da un client a un server. Il protocollo SMTP è composto da un insieme di regole con cui

viene gestita l'interazione tra un programma che invia i messaggi e un programma che li riceve. Una volta che un server ha ricevuto dei messaggi via SMTP, li conserva finché non vengono ritirati da un client mediante il protocollo POP, IMAP o altro.

Il sistema SMTP viene descritto nella RFC-2821, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc2821.txt

Spam - Posta indesiderata su Internet. Il termine "spam" viene generalmente utilizzato per indicare messaggi collettivi non richiesti e non desiderati. Si definisce "spammer" colui che, dopo aver ottenuto migliaia o centinaia di migliaia di indirizzi e-mail da varie fonti, utilizza tali indirizzi per inviare messaggi o richieste di vario tipo. Con "spam" si indica anche la pubblicazione di messaggi non richiesti o contenenti annunci pubblicitari non correlati alla discussione nell'ambito di un newsgroup o un forum di discussione pubblica.

Il fenomeno legato allo spamming è ormai diventato un problema, perché comporta notevoli sprechi di tempo e risorse server. Gli spammer usano tecniche molto diverse e sofisticate per tentare di mascherare l'origine dei propri messaggi, ad esempio utilizzando gli indirizzi e-mail altrui o inoltrando lo spam in modo occulto attraverso più server di posta. La prevenzione di questo fenomeno si rivela pertanto alquanto difficile. Il server MDaemon di Alt-N Technologies è dotato di numerose funzioni appositamente progettate per impedire lo spamming, ad esempio le liste nere DNS, lo scudo IP, il vaglio IP, il controllo dell'inoltro e altre.

L'origine del termine "spam" è ancora oggetto di discussione. Secondo la versione più accreditata, deriva da un famoso sketch del gruppo comico inglese Monty Python in cui la parola "spam" viene continuamente ripetuta e periodicamente accompagnata da un coro di Vichinghi che canta "Spam spam spam spam, spam spam spam spam...". Tuttavia, qualcuno afferma che si tratti semplicemente di un paragone poco lusinghiero con la carne in scatola Spam della Hormel, che, secondo un'opinione diffusa negli Stati Uniti, tutti prima o poi mangiano, anche se a nessuno piace.

TCP/IP - Acronimo di **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol. Il protocollo TCP/IP viene definito come la struttura fondamentale di Internet. Si tratta della suite di protocolli di comunicazione utilizzati per connettere gli host sia su Internet che sulle reti LAN. È un sistema a due livelli: quello superiore, TCP, gestisce il disassemblaggio e l'assemblaggio dei file in pacchetti per la trasmissione sulla rete; quello inferiore, IP, gestisce l'indirizzamento dei pacchetti in modo che raggiungano la destinazione corretta. I protocolli TCP e IP vengono discussi rispettivamente nella RFC-793 e nella RFC-791, consultabili su Internet agli indirizzi:

TCP - http://www.rfc-editor.org/rfc/rfc793.txt

IP - http://www.rfc-editor.org/rfc/rfc791.txt

Telnet - Comando e programma utilizzati per collegarsi ai siti Internet che supportano l'accesso Telnet. Tramite il comando Telnet, l'utente visualizza il prompt di accesso del server Telnet. Se l'utente dispone di un account su tale server, può accedere alle risorse autorizzate (file, messaggi e-mail e così via). Telnet presenta dei limiti: si tratta infatti di un programma da riga di comando che utilizza i comandi Unix.

Il protocollo TELNET viene descritto nelle RFC 854-855, consultabili su Internet agli indirizzi seguenti:

http://www.rfc-editor.org/rfc/rfc854.txt

http://www.rfc-editor.org/rfc/rfc855.txt

Terminale - Dispositivo che consente di inviare comandi a un computer remoto, ad esempio una tastiera, uno schermo, un circuito semplice, nonché un computer in emulazione.

Tiff - Acronimo di **T**agged **I**mage **F**ile **F**ormat. Si tratta di un formato di file grafico creato per fungere da convertitore grafico universale tra più piattaforme di elaborazione. Il formato TIFF è in grado di gestire intensità di colore da 1 a 24 bit.

UDP - Acronimo di **U**ser **D**atagram **P**rotocol . È uno dei protocolli che compongono la suite di protocolli TCP/IP per il trasferimento dei dati. Il protocollo UDP è noto come protocollo senza stato, poiché non riconosce l'avvenuta ricezione dei pacchetti inviati.

Il protocollo UDP viene descritto nella RFC-768, consultabile su Internet all'indirizzo

http://www.rfc-editor.org/rfc/rfc768.txt

Unix - Anche UNIX. Sistema operativo creato da Bell Labs negli anni Sessanta. Progettato per essere utilizzato da più utenti contemporaneamente, rappresenta il sistema operativo più popolare per i server su Internet. Esistono ormai molti sistemi operativi basati su UNIX: Linux, GNU, Ultrix, XENIX e altri.

URL - Acronimo di **U**niform **R**esource **L**ocator. Ogni file o server su Internet è dotato di un URL, ovvero dell'indirizzo che gli utenti immettono nel browser Web per accedere al file o al server in questione. Gli URL non possono contenere spazi e utilizzano sempre le barre normali (/). Sono costituiti da due parti, separate da "://": la prima rappresenta il protocollo utilizzato o la risorsa a cui ci si collega, ad esempio http, telnet, ftp e così via, mentre la seconda è l'indirizzo Internet del file o server, ad esempio www.altn.com o 127.0.0.1.

Uuencode - Set di algoritmi utilizzato per convertire i file in una serie di caratteri ASCII a 7 bit per la trasmissione su Internet. Nonostante rappresenti l'abbreviazione di Unix-to-Unix Encode (codifica da Unix a Unix), Uuencode non è più un protocollo esclusivo del sistema UNIX, ma è diventato universale. Consente la trasmissione di file tra piattaforme diverse. Si tratta di un metodo di codifica utilizzato comunemente nella posta elettronica.

WAN - Acronimo di **W**ide **A**rea **N**etwork. Una rete WAN è analoga a una LAN (Local Area Network), ma in genere si estende tra più edifici o città. Le reti WAN sono spesso costituite da LAN di dimensioni più piccole interconnesse. Internet può essere descritta come la più grande WAN del mondo.

Zip - Si riferisce a un file compresso o "zippato", contraddistinto di solito dall'estensione "`.zip`". Per estensione, "zippare" significa comprimere uno o più file in un unico file di archivio. Questa procedura consente di risparmiare spazio o di effettuare un trasferimento più rapido a un altro computer. Per utilizzare un file zip, è necessario decomprimerlo con un apposito programma, quale PKZIP o WinZip. Molti

siti Web consentono di scaricare utilità di compressione/decompressione, sia shareware che freeware.

Indice

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- L -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -